Export Report

Item 1:

- RiskId: 2907
- ComplianceId: 3347
- RiskTitle: Mismatched Employee Details Risk
- Criticality: High
- PossibleDamage: Inaccurate EPF data submission and compliance issues
- Category: Operational
- RiskType: Current
- BusinessImpact: All business units submitting EPF data
- RiskDescription: Mismatched employee details can lead to incorrect EPF contributions, penalties, and
- RiskLikelihood: 7
- RiskImpact: 9
- RiskExposureRating: 63
- RiskMultiplierX: 0.1
- RiskMultiplierY: 0.1
- RiskPriority: High
- RiskMitigation: {"1": "Regularly verify employee details against official records", "2": "Implement data va
- CreatedAt: 2025-12-02 00:00:00
- CreatedBy: System
- CreatedByName: System User
- DepartmentName: Information Security
- BusinessUnitName: Retail Banking

Item 2:

- RiskId: 2922
- ComplianceId: 2
- RiskTitle: risk title
- Criticality: Medium
- PossibleDamage: Potential data breaches due to unaddressed vulnerabilities
- Category: Process Risk
- RiskType: Current
- BusinessImpact: Revenue Loss
- RiskDescription: description riskk
- RiskLikelihood: 1

RiskImpact: 1
RiskExposureRating: 0.08
RiskMultiplierX: 0.2
RiskMultiplierY: 0.4
RiskPriority: Medium
RiskMitigation: sssssssssss■ssssssss
CreatedAt: 2025-12-02 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 3:
RiskId: 2921
ComplianceId: 3361
RiskTitle: Non-Retention of EPFO Correspondence
Criticality: High
PossibleDamage: Penalties, fines, legal actions
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal consequences and financial losses
RiskDescription: Failure to retain EPFO correspondence may result in non-compliance with EPF regula
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update stored correspondence", "2": "Implement access cor
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 4:
RiskId: 2920

ComplianceId: 3360
RiskTitle: Inaccurate Attendance Records
Criticality: High
PossibleDamage: Discrepancies in wage calculations and legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Financial losses and legal liabilities
RiskDescription: Inaccurate attendance records can result in discrepancies in wage calculations, leadi
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement biometric attendance systems for accurate tracking", "2": "Regular rec
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 5:
RiskId: 2919
ComplianceId: 3359
RiskTitle: Inaccurate Wage Records
Criticality: High
PossibleDamage: Penalties from EPF authorities and legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Financial losses and damage to reputation
RiskDescription: Inaccurate wage records can result in underpayment or overpayment of wages, leadi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits of wage registers to ensure accuracy", "2": "Employee training on

CreatedAt: 2025-12-02 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 6:

RiskId: 2918

ComplianceId: 3358

RiskTitle: Legal Penalties due to Inaccurate Documentation

Criticality: High

PossibleDamage: Legal fines, penalties, and reputational damage

Category: Compliance

RiskType: Inherent

BusinessImpact: Financial loss and damage to reputation

RiskDescription: Failure to retain accurate documentation of EPF contributions may lead to legal penal

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits of retained documents", "2": "Training finance staff on proper docu

CreatedAt: 2025-12-02 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 7:

RiskId: 2917

ComplianceId: 3357

RiskTitle: Non-compliance with Form Maintenance Requirements

Criticality: High

PossibleDamage: Penalties from EPF authorities, legal implications, reputational damage

Category: Compliance
RiskType: Residual
BusinessImpact: Potential financial losses, legal disputes, and damage to the organization's reputation
RiskDescription: Failure to maintain required forms may result in regulatory fines, legal actions, and ne
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure compliance", "2": "Employee training on form maintenan
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 8:
RiskId: 2916
ComplianceId: 3356
RiskTitle: Penalties for Non-Compliance
Criticality: High
PossibleDamage: Financial losses and legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses and legal consequences due to non-compliance.
RiskDescription: Failure to maintain accurate records, file returns on time, and comply with EPF regula
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly audit and reconcile records to ensure accuracy", "2": "Implement autom
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 9:

RiskId: 2915
ComplianceId: 3355
RiskTitle: Late Filing Compounding Fees Risk
Criticality: High
PossibleDamage: Financial penalties, reputation damage, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: All business units under EPF coverage
RiskDescription: Failure to submit EPF returns on time may result in financial penalties and non-compl
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set up reminders for filing deadlines", "2": "Implement automated submission proc
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 10:

RiskId: 2914
ComplianceId: 3354
RiskTitle: Legal Penalties for Non-Compliance
Criticality: High
PossibleDamage: Legal penalties, fines, or sanctions for failing to maintain required records
Category: Compliance
RiskType: Residual
BusinessImpact: Potential financial losses and damage to reputation
RiskDescription: Non-compliance with record-keeping requirements may result in regulatory penalties a

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular record update procedures", "2": "Provide training on record-ke
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 11:
RiskId: 2913
ComplianceId: 3353
RiskTitle: Penalties for Late EPF Contribution Filing
Criticality: High
PossibleDamage: Accrual of compounding fees and penalties
Category: Financial
RiskType: Inherent
BusinessImpact: Financial losses due to penalties and fees
RiskDescription: Failure to file EPF contributions on time may result in financial penalties and fees imp
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set up automated reminders for contribution deadlines", "2": "Implement a system
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 12:
RiskId: 2912

ComplianceId: 3352
RiskTitle: Inaccurate Employee Details
Criticality: High
PossibleDamage: Non-compliance penalties, legal disputes
Category: Operational
RiskType: Current
BusinessImpact: Delayed EPF processing, financial losses
RiskDescription: Incorrect employee details can lead to incorrect EPF contributions and legal disputes
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR staff on data verification processes", "2": "Automate emplo
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 13:
RiskId: 2911
ComplianceId: 3351
RiskTitle: Inaccurate Recordkeeping
Criticality: High
PossibleDamage: Penalties, fines, or legal actions by EPFO
Category: Operational
RiskType: Current
BusinessImpact: May lead to financial losses and damage to reputation
RiskDescription: Failure to maintain accurate records as per EPF requirements may result in penalties
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training for employees on recordkeeping procedures", "2": "Implement au

CreatedAt: 2025-12-02 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 14:

RiskId: 2910

ComplianceId: 3350

RiskTitle: Non-Compliance Identification

Criticality: Medium

PossibleDamage: Penalties, reputational damage, legal actions

Category: Operational

RiskType: Current

BusinessImpact: Financial losses, legal consequences

RiskDescription: Lack of regular monitoring may result in non-compliance issues going unnoticed, lead

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement regular compliance audits", "2": "Establish clear communication chann

CreatedAt: 2025-12-02 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 15:

RiskId: 2909

ComplianceId: 3349

RiskTitle: Late Submission of Documents

Criticality: High

PossibleDamage: Penalties, reputational damage, legal actions

Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal consequences
RiskDescription: Failure to adhere to filing deadlines may result in penalties imposed by EPFO, leading
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set up reminders for filing deadlines", "2": "Implement automated filing systems",
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 16:
RiskId: 2908
ComplianceId: 3348
RiskTitle: EPF Contribution Calculation Risk
Criticality: High
PossibleDamage: Financial discrepancies and compliance issues due to incorrect contribution calculat
Category: Operational
RiskType: Current
BusinessImpact: All business units calculating EPF contributions
RiskDescription: Incorrect EPF contribution calculations can result in financial discrepancies, penalties
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated calculation tools", "2": "Regularly review contribution calcul
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 17:

RiskId: 2892
ComplianceId: 3332
RiskTitle: Delayed Processing of Form 19
Criticality: Medium
PossibleDamage: Delayed fund settlement, legal implications
Category: Compliance
RiskType: Inherent
BusinessImpact: HR operations may be affected, employee relations may suffer
RiskDescription: Failure to process Form 19 within the specified timeline may lead to delayed fund sett
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated workflow for form processing", "2": "Regular monitoring of pending exi
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 18:

RiskId: 2906
ComplianceId: 3346
RiskTitle: Inaccurate EPF Contributions
Criticality: High
PossibleDamage: Incorrect EPF contributions leading to penalties, fines, and legal consequences
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units contributing to EPF
RiskDescription: Failure to verify EPF contributions accurately may result in financial penalties, legal lia

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR and finance teams on EPF contribution verification proces
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 19:
RiskId: 2905
ComplianceId: 3345
RiskTitle: Penalties for Non-compliance with EPF Annual Returns Filing
Criticality: High
PossibleDamage: Penalties, fines, or legal actions by regulatory authorities
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial loss and damage to reputation
RiskDescription: Failure to submit EPF annual returns accurately and on time may result in penalties, f
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set up reminders for annual return filing deadlines", "2": "Regularly review and re
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 20:
RiskId: 2904

ComplianceId: 3344
RiskTitle: Incorrect Information in Form 6A
Criticality: Medium
PossibleDamage: Incorrect contributions, penalties, legal actions
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial losses, legal implications
RiskDescription: Inaccurate information in Form 6A may lead to incorrect contributions, penalties, or le
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement data validation checks before submission", "2": "Regularly audit and re
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 21:
RiskId: 2903
ComplianceId: 3343
RiskTitle: Penalties for late or inaccurate Form 6A submission
Criticality: High
PossibleDamage: Penalties, fines, legal actions
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial losses, legal implications
RiskDescription: Late or inaccurate Form 6A submission may lead to penalties, fines, or legal actions b
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Set up reminders and alerts for Form 6A submission deadlines", "2": "Implement a

CreatedAt: 2025-12-02 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 22:

RiskId: 2902

ComplianceId: 3342

RiskTitle: Data Accuracy Issues

Criticality: Medium

PossibleDamage: Incorrect provident fund calculations, legal disputes

Category: Operational

RiskType: Current

BusinessImpact: Financial losses, legal liabilities

RiskDescription: Submission of inaccurate establishment and employee-wise details may result in inco

RiskLikelihood: 7

RiskImpact: 6

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement data validation checks before submission", "2": "Regularly review and

CreatedAt: 2025-12-02 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 23:

RiskId: 2901

ComplianceId: 3341

RiskTitle: Penalties for Non-compliance

Criticality: High

PossibleDamage: Financial penalties, legal actions

Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal liabilities
RiskDescription: Failure to submit Form 3A on time or with incorrect details may result in penalties and
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set up reminders for submission deadlines", "2": "Regularly update establishment
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 24:
RiskId: 2900
ComplianceId: 3340
RiskTitle: Legal Disputes over Contribution Details
Criticality: Medium
PossibleDamage: Legal liabilities due to inaccurate reporting
Category: Operational
RiskType: Current
BusinessImpact: Financial and reputational damage from legal disputes
RiskDescription: Inaccurate reporting of contribution details may lead to legal disputes with employees
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular audits of contribution data", "2": "Training on accurate reporting procedur
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 25:
RiskId: 2899
ComplianceId: 3339
RiskTitle: Penalties for Late Submission
Criticality: High
PossibleDamage: Financial penalties from EPF authorities
Category: Operational
RiskType: Current
BusinessImpact: Financial loss due to penalties
RiskDescription: Failure to submit annual returns by the deadline may result in financial penalties impo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear submission deadlines and reminders", "2": "Implement automated
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 26:
RiskId: 2898
ComplianceId: 3338
RiskTitle: Non-Issuance of PF Statement
Criticality: Medium
PossibleDamage: Legal non-compliance and employee dissatisfaction
Category: Operational
RiskType: Current
BusinessImpact: Employees may face difficulties in accessing their PF details, leading to dissatisfactio
RiskDescription: Failure to provide the PF statement to exiting employees can result in non-compliance

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Include PF statement issuance in the exit checklist for departing employees", "2":
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 27:
RiskId: 2897
ComplianceId: 3337
RiskTitle: Delayed Processing of Final Settlements
Criticality: High
PossibleDamage: Legal disputes and financial penalties due to delayed final settlements
Category: Operational
RiskType: Current
BusinessImpact: Delayed processing can lead to disgruntled employees and regulatory non-compliand
RiskDescription: Failure to process final settlements within the required timeframe can result in legal co
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear internal timelines for processing final settlements", "2": "Regularly
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 28:
RiskId: 2896

ComplianceId: 3336
RiskTitle: Delayed PF transfers
Criticality: Medium
PossibleDamage: Penalties for delayed transfers, legal implications
Category: Operational
RiskType: Inherent
BusinessImpact: Financial penalties, legal consequences
RiskDescription: Failure to process Form 31 for PF transfer within the stipulated time may lead to delay
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated reminders for PF transfer processing", "2": "Regular monitoring of pen
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 29:
RiskId: 2895
ComplianceId: 3335
RiskTitle: Delay in processing employee benefits
Criticality: High
PossibleDamage: Financial loss due to delayed benefits processing
Category: Operational
RiskType: Inherent
BusinessImpact: Delayed benefits disbursement, employee dissatisfaction
RiskDescription: If Form 2 is not collected on time, there may be delays in processing employee benefi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Automated reminders for form submission deadlines", "2": "Regular follow-ups wit

CreatedAt: 2025-12-02 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 30:

RiskId: 2894

ComplianceId: 3334

RiskTitle: Late Submission of PF Returns

Criticality: High

PossibleDamage: Penalties, legal consequences

Category: Operational

RiskType: Current

BusinessImpact: Financial penalties, legal liabilities

RiskDescription: Failure to submit PF returns on time can result in penalties and legal consequences fo

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Set up reminders for submission deadlines", "2": "Regular audits of submission pr

CreatedAt: 2025-12-02 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 31:

RiskId: 2893

ComplianceId: 3333

RiskTitle: Delayed PF Contributions

Criticality: High

PossibleDamage: Penalties, legal issues, employee dissatisfaction

Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal liabilities, employee morale
RiskDescription: Failure to make timely PF contributions can result in penalties, legal consequences, a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate contribution tracking system", "2": "Regular training for responsible pers
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 32:
RiskId: 2891
ComplianceId: 3331
RiskTitle: Delayed Submission of Form 2
Criticality: High
PossibleDamage: Financial penalties, compliance issues
Category: Compliance
RiskType: Inherent
BusinessImpact: HR operations may be affected, financial penalties may be incurred
RiskDescription: Failure to collect and submit Form 2 within the specified timeline may result in compli
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR personnel on form collection procedures", "2": "Automated
CreatedAt: 2025-12-02 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 33:
RiskId: 2884
ComplianceId: 3324
RiskTitle: Loss of Compliance Records
Criticality: High
PossibleDamage: Loss of critical compliance records may lead to severe penalties, legal consequence
Category: Compliance
RiskType: Residual
BusinessImpact: Loss of critical compliance records could result in non-compliance fines, legal actions
RiskDescription: The risk of losing compliance records poses a significant threat to the organization's a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular data backups to prevent loss of records", "2": "Implement access controls
CreatedAt: 2025-12-01 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 34:
RiskId: 2885
ComplianceId: 3325
RiskTitle: Non-Compliance Penalties
Criticality: High
PossibleDamage: Financial penalties, legal actions, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Potential financial losses and damage to company reputation
RiskDescription: Failure to meet statutory deadlines could result in penalties and legal consequences.

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication channels for deadline updates", "2": "Implement au
CreatedAt: 2025-12-01 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 35:
RiskId: 2886
ComplianceId: 3326
RiskTitle: Legal Non-Compliance Risk
Criticality: High
PossibleDamage: Legal penalties, fines, or reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to comply with training requirements may lead to legal actions, financial losses
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update training materials to reflect current regulations", "2": "Provide ref
CreatedAt: 2025-12-01 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 36:
RiskId: 2887

ComplianceId: 3327
RiskTitle: Legal Non-Compliance Risk due to Law Changes
Criticality: High
PossibleDamage: Legal penalties, fines, or reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to comply with training on new legal requirements may lead to legal actions, fi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide timely updates on legal changes", "2": "Conduct targeted training session
CreatedAt: 2025-12-01 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 37:
RiskId: 2759
ComplianceId: 3206
RiskTitle: Delayed Gratuity Payments
Criticality: High
PossibleDamage: Legal disputes, employee dissatisfaction, financial penalties
Category: Operational
RiskType: Current
BusinessImpact: HR and Legal departments
RiskDescription: Failure to timely disburse gratuity to fixed-term employees can result in legal disputes
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement automated reminders for payment deadlines", "2": "Regularly review a

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 38:

RiskId: 2760

ComplianceId: 3207

RiskTitle: Late Gratuity Payments

Criticality: Medium

PossibleDamage: Legal non-compliance, financial penalties, employee dissatisfaction

Category: Operational

RiskType: Current

BusinessImpact: HR and Legal departments

RiskDescription: Failure to process gratuity payments within the specified timeline can lead to legal no

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement automated reminders for payment deadlines", "2": "Establish clear co

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 39:

RiskId: 2761

ComplianceId: 3208

RiskTitle: Inaccurate Contribution Calculation

Criticality: High

PossibleDamage: Legal penalties, reputational damage, and insufficient funding for re-skilling initiative

Category: Operational
RiskType: Inherent
BusinessImpact: Financial loss and damage to organizational reputation
RiskDescription: Incorrect contribution calculations may lead to legal consequences and inadequate su
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular audits to verify contribution calculations", "2": "Provide training
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 40:
RiskId: 2762
ComplianceId: 3209
RiskTitle: Late Contribution to Re-skilling Fund
Criticality: Medium
PossibleDamage: Penalties, delays in re-skilling initiatives, and inadequate support for retrenched emp
Category: Operational
RiskType: Inherent
BusinessImpact: Financial penalties and negative impact on employee welfare
RiskDescription: Delayed contributions may result in penalties and hinder the timely support for retrenc
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Set up reminders and alerts for contribution deadlines", "2": "Establish clear comm
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 41:
RiskId: 2763
ComplianceId: 3210
RiskTitle: Delay in Forming Negotiating Council
Criticality: High
PossibleDamage: Disputes, lack of representation, hindered negotiation process
Category: Operational
RiskType: Current
BusinessImpact: HR operations, labor relations
RiskDescription: Failure to form the Negotiating Council within the specified timeframe may lead to cor
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set clear timelines and responsibilities for HR to facilitate the formation process",
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 42:
RiskId: 2764
ComplianceId: 3211
RiskTitle: Delayed Registration
Criticality: High
PossibleDamage: Legal penalties, operational disruptions, loss of business opportunities
Category: Operational
RiskType: Inherent
BusinessImpact: Potential delays in commencing operations and legal consequences
RiskDescription: Failure to submit the registration application within the specified timeframe may lead t

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear submission guidelines and deadlines", "2": "Provide support for do
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 43:
RiskId: 2765
ComplianceId: 3212
RiskTitle: Incomplete Registration Acknowledgment
Criticality: Medium
PossibleDamage: Operational uncertainties, potential delays in compliance verification
Category: Operational
RiskType: Inherent
BusinessImpact: Uncertainty regarding the completion of registration process and potential compliance
RiskDescription: Failure to receive confirmation of registration may lead to operational uncertainties an
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels for issue resolution", "2": "Regularly mon
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 44:
RiskId: 2766

ComplianceId: 3213
RiskTitle: Biased Decision-Making in Safety Committees
Criticality: High
PossibleDamage: Ineffective safety measures and increased risk of accidents
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units with 500 or more employees
RiskDescription: Lack of balanced representation in safety committees may result in biased decisions t
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear selection criteria for committee members", "2": "Provide diversity t
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 45:
RiskId: 2767
ComplianceId: 3214
RiskTitle: Delayed Formation of Safety Committees
Criticality: Medium
PossibleDamage: Unaddressed safety concerns and increased risks
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units with 500 or more employees
RiskDescription: Delay in establishing safety committees may result in safety issues going unaddresse
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Develop a clear timeline for committee formation", "2": "Allocate resources for cor

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 46:

RiskId: 2768

ComplianceId: 3215

RiskTitle: Non-Submission of Annual Declaration

Criticality: High

PossibleDamage: Legal penalties, reputational damage

Category: Compliance

RiskType: Inherent

BusinessImpact: Financial losses, legal consequences

RiskDescription: Failure to submit the annual declaration may lead to legal penalties, reputational dam

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish a reminder system for HR to submit declarations on time", "2": "Provide

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 47:

RiskId: 2769

ComplianceId: 3206

RiskTitle: Delayed Gratuity Payments

Criticality: High

PossibleDamage: Legal disputes, employee dissatisfaction, and reputational damage

Category: Operational
RiskType: Current
BusinessImpact: Potential legal costs, loss of employee trust, and damage to employer reputation
RiskDescription: Failure to disburse gratuity within the stipulated timeframe may lead to legal claims fro
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of gratuity payments", "2": "Implement automated reminders for pa
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 48:
RiskId: 2770
ComplianceId: 3207
RiskTitle: Inaccurate Employee Tenure Tracking
Criticality: Medium
PossibleDamage: Incorrect gratuity payments and legal disputes
Category: Operational
RiskType: Current
BusinessImpact: Financial losses due to incorrect payments and potential legal costs
RiskDescription: Failure to accurately track employee tenure may result in incorrect gratuity payments,
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement centralized HRIS system for accurate records", "2": "Regularly update
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 49:
RiskId: 2771
ComplianceId: 3208
RiskTitle: Non-Compliance with Contribution Requirement
Criticality: High
PossibleDamage: Legal penalties and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal disputes and financial losses
RiskDescription: Failure to contribute to the Re-skilling Fund as required by regulations may result in le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of contribution deadlines", "2": "Training for finance departmer
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 50:
RiskId: 2772
ComplianceId: 3209
RiskTitle: Mismanagement of Re-skilling Fund
Criticality: Medium
PossibleDamage: Financial discrepancies and legal issues
Category: Financial
RiskType: Current
BusinessImpact: Financial losses and regulatory scrutiny
RiskDescription: Inaccurate calculation and transfer of contributions to the Re-skilling Fund may lead to

RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Training for finance departments on fund management procedures", "2": "Implem
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 51:
RiskId: 2773
ComplianceId: 3210
RiskTitle: Inaccurate Union Membership Verification
Criticality: High
PossibleDamage: Legal disputes, loss of union recognition, labor unrest
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal costs, loss of workforce representation
RiskDescription: Failure to accurately verify union membership leading to disputes and potential loss o
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR and auditors on verification process", "2": "Implement auto
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 52:
RiskId: 2774

ComplianceId: 3211
RiskTitle: Non-Compliance with Electronic Registration
Criticality: High
PossibleDamage: Legal penalties and fines for non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Financial losses and reputational damage
RiskDescription: Failure to register electronically may lead to legal actions by regulatory authorities, res
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication of registration requirements and deadlines to all esta
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 53:
RiskId: 2775
ComplianceId: 3212
RiskTitle: Data Breach Due to Lack of Encryption
Criticality: High
PossibleDamage: Loss of confidential information, reputational damage
Category: IT
RiskType: Inherent
BusinessImpact: IT systems, reputation of the Ministry
RiskDescription: Failure to encrypt registration data may lead to unauthorized access, data breaches, a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update encryption protocols", "2": "Implement multi-factor authentication

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 54:

RiskId: 2776

ComplianceId: 3213

RiskTitle: Data Corruption Due to Lack of Audits

Criticality: Medium

PossibleDamage: Data loss, compliance violations

Category: Operational

RiskType: Inherent

BusinessImpact: IT systems, data integrity

RiskDescription: Failure to conduct regular database audits may result in undetected data corruption, u

RiskLikelihood: 6

RiskImpact: 8

RiskExposureRating: 48

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement automated auditing tools", "2": "Train IT staff on audit procedures", "3"

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 55:

RiskId: 2777

ComplianceId: 3214

RiskTitle: Undetected Health Issues in Employees

Criticality: High

PossibleDamage: Employees may suffer from untreated health conditions leading to absenteeism and

Category: Operational
RiskType: Inherent
BusinessImpact: Decreased productivity, increased healthcare costs, and potential legal liabilities.
RiskDescription: Failure to schedule annual health check-ups may result in employees developing seri
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reminder system for HR departments", "2": "Provide incenti
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 56:
RiskId: 2778
ComplianceId: 3215
RiskTitle: Inaccurate Health Assessments by Non-Accredited Providers
Criticality: Medium
PossibleDamage: Employees may receive incorrect health assessments leading to inappropriate treatr
Category: Operational
RiskType: Inherent
BusinessImpact: Compromised employee health, potential legal issues, and decreased trust in employ
RiskDescription: Partnering with non-accredited healthcare providers may result in inaccurate health as
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear criteria for selecting healthcare providers", "2": "Regularly review p
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 57:
RiskId: 2779
ComplianceId: 3216
RiskTitle: Failure to Establish Safety Committees
Criticality: High
PossibleDamage: Increased workplace accidents, legal penalties, and reputational harm
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, increased insurance costs, potential lawsuits
RiskDescription: Failure to establish safety committees as required may result in inadequate safety me
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely formation of safety committees as per policy requirements", "2": "Pr
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 58:
RiskId: 2780
ComplianceId: 3217
RiskTitle: Non-compliance with Quarterly Reporting
Criticality: High
PossibleDamage: Fines, legal actions, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Legal consequences, financial penalties
RiskDescription: Failure to report accurate migrant worker numbers quarterly may result in legal action

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR staff on reporting requirements", "2": "Internal audits to ve
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 59:
RiskId: 2781
ComplianceId: 3218
RiskTitle: Lack of Training on Declaration Process
Criticality: Medium
PossibleDamage: Inaccurate reporting, non-compliance
Category: Compliance
RiskType: Current
BusinessImpact: Risk of non-compliance, legal actions
RiskDescription: Failure to provide adequate training on the declaration process of migrant workers ma
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop comprehensive training modules on migrant worker declaration process"
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 60:
RiskId: 2782

ComplianceId: 3219
RiskTitle: Non-compliance with Annual Travel Allowance Provision
Criticality: High
PossibleDamage: Financial penalties, legal repercussions, negative impact on employer reputation
Category: Operational
RiskType: Residual
BusinessImpact: Delayed or missed payments leading to dissatisfaction among migrant workers, poter
RiskDescription: Failure to provide annual travel allowances to migrant workers as per regulations may
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear guidelines and timelines for travel allowance disbursement", "2": "I
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 61:
RiskId: 2783
ComplianceId: 3220
RiskTitle: Non-compliance with Social Security Access for Migrant Workers
Criticality: High
PossibleDamage: Legal liabilities, financial penalties, negative impact on employer reputation
Category: Operational
RiskType: Residual
BusinessImpact: Migrant workers being deprived of social security benefits, potential legal actions aga
RiskDescription: Failure to provide access to social security systems for migrant workers may lead to le
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Provide comprehensive training to HR staff on social security benefit administrati

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 62:

RiskId: 2784

ComplianceId: 3221

RiskTitle: Non-Compliance with Timely Processing of Wage Payments

Criticality: High

PossibleDamage: Legal penalties, employee dissatisfaction, reputational damage

Category: Operational

RiskType: Current

BusinessImpact: Financial losses, legal disputes, damaged reputation

RiskDescription: Failure to process wage payments on time may result in legal consequences, employ

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement automated reminders for payment deadlines", "2": "Regularly audit pay

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 63:

RiskId: 2785

ComplianceId: 3222

RiskTitle: Non-Compliance with Monthly Record-Keeping of Wage Payments

Criticality: Medium

PossibleDamage: Compliance violations, audit issues, financial discrepancies

Category: Operational
RiskType: Current
BusinessImpact: Financial losses, audit penalties, compliance violations
RiskDescription: Failure to update wage payment records timely may result in compliance violations, a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated record-keeping systems", "2": "Regularly review and recon
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 64:
RiskId: 2786
ComplianceId: 3223
RiskTitle: Non-Enrollment of Eligible Employees
Criticality: High
PossibleDamage: Legal penalties, loss of benefits for employees, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to enroll eligible employees in social security schemes within the specified tim
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure timely enrollment", "2": "Training HR staff on enrollment
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 65:
RiskId: 2787
ComplianceId: 3224
RiskTitle: Workplace Safety Incidents
Criticality: High
PossibleDamage: Increased workplace accidents, injuries, or legal liabilities
Category: Operational
RiskType: Inherent
BusinessImpact: Potential harm to employees, financial losses, and damage to the organization's repu
RiskDescription: Failure to provide adequate health and safety training may lead to workplace incident
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly scheduled training sessions", "2": "Provide refresher courses throughou
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 66:
RiskId: 2788
ComplianceId: 3225
RiskTitle: Ineffective Grievance Resolution
Criticality: High
PossibleDamage: Delayed resolution of grievances, worker dissatisfaction, legal implications
Category: Operational
RiskType: Current
BusinessImpact: Potential legal actions, negative impact on worker morale and productivity
RiskDescription: Failure to address grievances through the helpline can lead to increased dissatisfacti

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for helpline operators on grievance handling", "2": "Establish clea
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 67:
RiskId: 2789
ComplianceId: 3226
RiskTitle: Delayed Helpline Implementation
Criticality: Medium
PossibleDamage: Unresolved grievances, worker dissatisfaction, negative impact on reputation
Category: Operational
RiskType: Current
BusinessImpact: Worker dissatisfaction, potential legal issues, negative publicity
RiskDescription: Failure to operationalize the helpline within the specified timeframe may lead to migra
RiskLikelihood: 5
RiskImpact: 8
RiskExposureRating: 40
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular progress reviews and updates on helpline setup", "2": "Allocate additiona
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 68:
RiskId: 2790

ComplianceId: 3227
RiskTitle: Data Security Breach
Criticality: High
PossibleDamage: Loss of sensitive worker information, compromised worker welfare tracking, legal im
Category: Operational
RiskType: Inherent
BusinessImpact: Ministry of Labor and Employment, state governments
RiskDescription: Unauthorized access to sensitive worker data or data breaches could lead to severe c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption measures for data security", "2": "Regularly update s
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 69:
RiskId: 2791
ComplianceId: 3228
RiskTitle: Workplace Safety Risks for Women Workers
Criticality: High
PossibleDamage: Increased risk of accidents or harm to women workers due to lack of safety protocols
Category: Operational
RiskType: Inherent
BusinessImpact: All business units with women workers
RiskDescription: Failure to implement safety protocols may lead to workplace accidents, injuries, or leg
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular safety audits to identify and address any safety gaps", "2": "Provide ongo

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 70:

RiskId: 2792

ComplianceId: 3229

RiskTitle: Miscommunication of Consent

Criticality: High

PossibleDamage: Legal disputes, employee dissatisfaction, potential lawsuits

Category: Compliance

RiskType: Inherent

BusinessImpact: HR departments and legal teams would need to allocate resources to address legal is

RiskDescription: Failure to properly communicate and document consent for night shifts could result in

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Provide detailed training on how to correctly fill out the consent form", "2": "Regula

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 71:

RiskId: 2793

ComplianceId: 3230

RiskTitle: Non-Compliance with Consent Management Practices

Criticality: Medium

PossibleDamage: Legal disputes, non-compliance penalties, reputational damage

Category: Compliance
RiskType: Inherent
BusinessImpact: Legal teams and HR departments would need to address non-compliance issues
RiskDescription: Failure to provide proper training on consent management practices could result in HR
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly conduct refresher training sessions on consent management practices"
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 72:
RiskId: 2794
ComplianceId: 3231
RiskTitle: Delay in Establishment of Social Security Fund
Criticality: High
PossibleDamage: Unavailability of benefits for unorganized workers
Category: Operational
RiskType: Inherent
BusinessImpact: Adverse impact on unorganized workers and public perception of the Ministry
RiskDescription: Failure to establish the fund within the specified timeline may lead to legal and social
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of fund establishment progress", "2": "Escalation process for a
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 73:
RiskId: 2795
ComplianceId: 3232
RiskTitle: Non-Compliance with Minimum Wage Laws
Criticality: High
PossibleDamage: Fines, legal actions, and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial penalties and damage to reputation
RiskDescription: Failure to comply with minimum wage laws may lead to legal actions, fines, and reput
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits and inspections", "2": "Training programs on minimum wage laws"
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 74:
RiskId: 2796
ComplianceId: 3233
RiskTitle: Ineffective Technology Utilization for Compliance Monitoring
Criticality: Medium
PossibleDamage: Inaccurate reporting and monitoring
Category: Operational
RiskType: Current
BusinessImpact: Non-compliance and potential penalties
RiskDescription: Ineffective use of technology for compliance monitoring may lead to inaccuracies in re

RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular updates and maintenance of technology systems", "2": "Employee trainin
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 75:
RiskId: 2797
ComplianceId: 3234
RiskTitle: Non-Compliance with Minimum Wage Laws
Criticality: High
PossibleDamage: Potential fines and legal actions
Category: Compliance
RiskType: Current
BusinessImpact: All business units employing workers under the New Labour Code
RiskDescription: Failure to conduct quarterly wage audits may result in non-compliance with minimum
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR departments on minimum wage laws", "2": "Automate auc
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 76:
RiskId: 2798

ComplianceId: 3235
RiskTitle: Inaccurate Leave Records
Criticality: High
PossibleDamage: Disputes, compliance violations, legal actions
Category: Operational
RiskType: Current
BusinessImpact: May lead to employee dissatisfaction, legal issues, and financial losses
RiskDescription: Failure to update leave records in real-time may result in inaccuracies, disputes, and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR personnel on leave record management procedures", "2":
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 77:
RiskId: 2799
ComplianceId: 3236
RiskTitle: Unreviewed Leave Records
Criticality: Medium
PossibleDamage: Errors, discrepancies, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: May lead to inaccurate employee entitlements, compliance issues, and disputes
RiskDescription: Failure to review leave records monthly may result in undetected errors, discrepancie
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish a standardized review process for leave records", "2": "Implement cross

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 78:

RiskId: 2800

ComplianceId: 3237

RiskTitle: Workplace Accident Risk

Criticality: High

PossibleDamage: Increased workplace accidents and potential legal liabilities.

Category: Operational

RiskType: Residual

BusinessImpact: Potential injuries to employees, property damage, and legal consequences.

RiskDescription: Lack of safety training may result in employees not knowing how to respond to workpl

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular safety training sessions", "2": "Provide safety equipment and signage", "3

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 79:

RiskId: 2801

ComplianceId: 3238

RiskTitle: Failure to Report Incidents

Criticality: High

PossibleDamage: Delayed response to critical incidents, potential harm to employees, and damage to

Category: Operational
RiskType: Inherent
BusinessImpact: May result in increased liability, reputational damage, and compromised employee sa
RiskDescription: Failure to report incidents in a timely manner can lead to serious consequences for th
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide regular training on incident reporting procedures", "2": "Implement autom
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 80:
RiskId: 2802
ComplianceId: 3239
RiskTitle: Late Incident Reporting
Criticality: Medium
PossibleDamage: Delayed incident response, compromised evidence, and increased legal exposure
Category: Operational
RiskType: Inherent
BusinessImpact: May result in incomplete investigations, compromised evidence, and increased legal
RiskDescription: Late incident reporting can hinder the organization's ability to address issues promptly
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated incident reporting reminders", "2": "Establish clear consequ
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 81:
RiskId: 2803
ComplianceId: 3240
RiskTitle: Non-compliance with Minimum Wage Review Process
Criticality: High
PossibleDamage: Legal disputes, strikes, and reputational damage
Category: Legal
RiskType: Inherent
BusinessImpact: Impact on Ministry of Labour and Employment operations and reputation
RiskDescription: Failure to conduct periodic reviews of minimum wages may lead to legal challenges, l
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Utilize economic data and stakeholder consultations for informed wage adjustmer
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 82:
RiskId: 2804
ComplianceId: 3241
RiskTitle: Financial Hardship for Employees
Criticality: High
PossibleDamage: Employees may struggle to meet financial obligations.
Category: Operational
RiskType: Current
BusinessImpact: Decreased employee morale and potential legal consequences.
RiskDescription: Delayed wage payments can lead to employee dissatisfaction and potential legal acti

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated payroll systems", "2": "Regularly review payment schedules
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 83:
RiskId: 2805
ComplianceId: 3242
RiskTitle: Legal Penalties and Employee Dissatisfaction
Criticality: High
PossibleDamage: Legal fines, loss of employee benefits, and damage to employer reputation.
Category: Compliance
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to comply with the employer contribution percentage requirement may lead to
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure compliance", "2": "Training programs for HR and payroll
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 84:
RiskId: 2806

ComplianceId: 3243
RiskTitle: Inadequate Worker Registration
Criticality: High
PossibleDamage: Workers being excluded from social security benefits
Category: Operational
RiskType: Inherent
BusinessImpact: Financial insecurity and potential social unrest among workers
RiskDescription: Failure to establish the national worker database portal may lead to workers in the un
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting on portal development progress", "2": "Engage
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 85:
RiskId: 2807
ComplianceId: 3244
RiskTitle: Delayed Database Operationalization
Criticality: High
PossibleDamage: Workers being excluded from social security benefits due to implementation delays
Category: Operational
RiskType: Inherent
BusinessImpact: Financial insecurity and potential social unrest among workers
RiskDescription: Failure to operationalize the national worker database within one year may lead to de
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear project timelines and milestones for database implementation", "2"

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 86:

RiskId: 2808

ComplianceId: 3245

RiskTitle: Undetected Health Issues in Employees

Criticality: High

PossibleDamage: Undiagnosed health issues may lead to decreased productivity, increased absentee

Category: Operational

RiskType: Inherent

BusinessImpact: Decreased productivity, increased absenteeism, potential legal liabilities.

RiskDescription: Failure to conduct annual health check-ups may result in undetected health issues in

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular health check-ups for employees", "2": "Promote health awareness and pr

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 87:

RiskId: 2809

ComplianceId: 3246

RiskTitle: Workplace Accident Risk

Criticality: High

PossibleDamage: Work-related injuries, legal liabilities, and reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, decreased productivity, and damage to company reputation
RiskDescription: Failure to provide adequate safety training may result in workplace accidents, injuries
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular safety training sessions", "2": "Safety drills and simulations", "3": "Inciden
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 88:
RiskId: 2810
ComplianceId: 3247
RiskTitle: Failure to establish 24/7 helpline
Criticality: High
PossibleDamage: Unresolved grievances and potential unrest among Inter-State Migrant Workers
Category: Operational
RiskType: Inherent
BusinessImpact: Ministry's reputation and credibility at risk
RiskDescription: If the helpline is not established, Inter-State Migrant Workers may face challenges in r
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of helpline operations", "2": "Training staff to handle grievance
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 89:
RiskId: 2811
ComplianceId: 3248
RiskTitle: Data Security and Accuracy Risk
Criticality: High
PossibleDamage: Potential exploitation and loss of welfare benefits for migrant workers
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of trust in government agencies, legal implications, financial losses
RiskDescription: Risk of unauthorized access, data breaches, and inaccurate data entries in the nation
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits and data validation processes", "2": "Encryption and access contro
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 90:
RiskId: 2812
ComplianceId: 3249
RiskTitle: Data Accuracy and Timeliness Risk
Criticality: Medium
PossibleDamage: Misinformed decisions and inadequate support for migrant workers
Category: Operational
RiskType: Inherent
BusinessImpact: Inefficiencies in resource allocation, delays in welfare benefits distribution, reduced tr
RiskDescription: Risk of outdated or incorrect data in the national database due to lack of regular upda

RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated data synchronization processes", "2": "Regular data quality checks an
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 91:
RiskId: 2813
ComplianceId: 3250
RiskTitle: Physical Harm to Women Employees during Night Shifts
Criticality: High
PossibleDamage: Risk of physical harm, assault, or injury to women employees
Category: Operational
RiskType: Inherent
BusinessImpact: All business units with women employees working night shifts
RiskDescription: The risk of physical harm to women employees during night shifts due to inadequate s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular safety training for employees", "2": "Installation of panic buttons or emerg
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 92:
RiskId: 2814

ComplianceId: 3251
RiskTitle: Legal Penalties for Non-Compliance
Criticality: High
PossibleDamage: Legal fines, lawsuits, and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal costs and damage to the company's reputation
RiskDescription: Failure to comply with maternity leave regulations may result in legal penalties, lawsu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the maternity leave policy to ensure compliance with
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 93:
RiskId: 2815
ComplianceId: 3252
RiskTitle: Safety Violations in Crèche Facility
Criticality: High
PossibleDamage: Legal fines, child safety issues, and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal costs and damage to the company's reputation
RiskDescription: Failure to maintain a safe and compliant crèche facility may result in legal penalties, c
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly inspect and maintain the cr\u00e8che facility to ensure compliance with
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 94:
RiskId: 2816
ComplianceId: 3253
RiskTitle: Undetected Workplace Hazards
Criticality: High
PossibleDamage: Increased likelihood of workplace accidents and injuries
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to conduct regular risk assessments may result in unidentified workplace haza
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement corrective actions based on assessment findings", "2": "Provide additio
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 95:
RiskId: 2817
ComplianceId: 3254
RiskTitle: Lack of Safety Training
Criticality: Medium
PossibleDamage: Lack of awareness leading to unsafe practices and incidents

Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to provide adequate safety training may result in employees being unaware of
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly schedule and conduct safety training sessions", "2": "Provide refresher
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 96:
RiskId: 2818
ComplianceId: 3255
RiskTitle: Delayed Grievance Resolution
Criticality: High
PossibleDamage: Decreased employee morale, potential legal actions, and negative impact on produc
Category: Operational
RiskType: Current
BusinessImpact: Delayed resolution of grievances affecting employee satisfaction and productivity.
RiskDescription: Failure to address grievances within the specified timeline may lead to increased diss
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of grievance resolution process", "2": "Timely training for Griev
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 97:
RiskId: 2819
ComplianceId: 3256
RiskTitle: Failure to Meet Grievance Resolution Timeline
Criticality: Medium
PossibleDamage: Decreased employee trust, potential legal actions, and negative impact on employee
Category: Operational
RiskType: Current
BusinessImpact: Failure to resolve grievances within the specified timeline may lead to decreased emp
RiskDescription: Not meeting the specified timeline for grievance resolution may result in increased dis
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update employees on grievance resolution progress", "2": "Implement a
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 98:
RiskId: 2820
ComplianceId: 3257
RiskTitle: Incorrect Overtime Calculation
Criticality: High
PossibleDamage: Underpayment of employees, legal disputes, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, legal expenses, employee dissatisfaction
RiskDescription: Incorrectly calculating overtime may result in employees not being compensated fairly

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of overtime calculations", "2": "Training for payroll staff on accurate
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 99:
RiskId: 2821
ComplianceId: 3258
RiskTitle: Delayed Overtime Payments
Criticality: Medium
PossibleDamage: Employee dissatisfaction, decreased morale, retention issues
Category: Operational
RiskType: Inherent
BusinessImpact: Decreased morale, potential retention issues, negative impact on productivity
RiskDescription: Delays in processing overtime payments may lead to employee dissatisfaction, decre
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate bi-weekly overtime processing", "2": "Regular monitoring of processing
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 100:
RiskId: 2822

ComplianceId: 3259
RiskTitle: Non-Compliance with Leave Application Process
Criticality: High
PossibleDamage: Staffing shortages, project delays, and decreased productivity
Category: Operational
RiskType: Residual
BusinessImpact: Significant impact on project timelines and operational efficiency
RiskDescription: Failure to adhere to the standardized leave application process could result in inadeq
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on the leave application process", "2": "Escalation proce
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 101:
RiskId: 2823
ComplianceId: 3260
RiskTitle: Legal Penalties for Late Wage Payments
Criticality: High
PossibleDamage: Legal fines, penalties, and reputation damage
Category: Legal
RiskType: Current
BusinessImpact: Financial losses and damage to employer reputation
RiskDescription: Non-compliance with wage payment regulations may result in legal consequences an
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement automated payroll systems to ensure timely payments", "2": "Regularly

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 102:

RiskId: 2824

ComplianceId: 3261

RiskTitle: Undetected Compliance Violations

Criticality: Medium

PossibleDamage: Regulatory fines and penalties

Category: Legal

RiskType: Current

BusinessImpact: Financial losses and legal consequences

RiskDescription: Failure to conduct quarterly compliance reviews may result in unnoticed violations and

RiskLikelihood: 7

RiskImpact: 6

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish a quarterly compliance review process", "2": "Document review findings

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 103:

RiskId: 2825

ComplianceId: 3262

RiskTitle: Non-Compliance with Employee Registration

Criticality: High

PossibleDamage: Legal penalties, employee dissatisfaction

Category: Compliance
RiskType: Current
BusinessImpact: HR, finance departments may face legal consequences and employee grievances
RiskDescription: Failure to register employees for social security benefits within the required timeframe
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set up automated reminders for HR to register new employees", "2": "Provide trai
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 104:
RiskId: 2826
ComplianceId: 3263
RiskTitle: Non-Compliance with Monthly Contributions
Criticality: High
PossibleDamage: Legal penalties, loss of employee benefits
Category: Compliance
RiskType: Current
BusinessImpact: HR, finance departments may face legal consequences and employee grievances
RiskDescription: Failure to make monthly contributions to social security funds may result in legal pena
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set up automated payment systems for contributions", "2": "Regularly reconcile co
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 105:
RiskId: 2827
ComplianceId: 3264
RiskTitle: Workplace Accidents Due to Lack of Training
Criticality: High
PossibleDamage: Increased workplace accidents and potential legal liabilities
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Employees may not be aware of workplace hazards and safety protocols, leading to a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training completion", "2": "Implementing consequences for
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 106:
RiskId: 2828
ComplianceId: 3265
RiskTitle: Delays in Dispute Resolution
Criticality: High
PossibleDamage: Delays in resolving disputes, increased backlog of cases, decreased trust in the tribu
Category: Operational
RiskType: Inherent
BusinessImpact: Potential legal challenges, decreased efficiency in resolving disputes, negative impac
RiskDescription: Failure to establish and follow case management procedures may lead to delays in re

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of case progress, escalation of delays to higher authorities", "
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 107:
RiskId: 2829
ComplianceId: 3266
RiskTitle: Data Security Breach
Criticality: High
PossibleDamage: Unauthorized access to sensitive migrant worker data
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of trust, legal implications, financial penalties
RiskDescription: Potential breach of the national database leading to unauthorized access to personal
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regular security assessments and up
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 108:
RiskId: 2830

ComplianceId: 3267
RiskTitle: Data Privacy Violation
Criticality: Medium
PossibleDamage: Unauthorized access to migrant worker data
Category: IT
RiskType: Inherent
BusinessImpact: Legal consequences, loss of trust
RiskDescription: Failure to safeguard migrant worker data leading to unauthorized access and potentia
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement access controls and user permissions", "2": "Regularly review and upd
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 109:
RiskId: 2831
ComplianceId: 3268
RiskTitle: Delay in Grievance Resolution
Criticality: High
PossibleDamage: Increased dissatisfaction and potential unrest among Inter-State Migrant Workers
Category: Operational
RiskType: Inherent
BusinessImpact: State Labor Departments and Ministry of Labor and Employment operations
RiskDescription: Failure to establish the helpline within the specified timeframe may result in unresolve
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular monitoring of helpline operations", "2": "Training of personnel to handle s

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 110:

RiskId: 2832

ComplianceId: 3269

RiskTitle: Unidentified Hazards and Risks

Criticality: High

PossibleDamage: Increased likelihood of accidents and injuries

Category: Operational

RiskType: Current

BusinessImpact: Potential legal liabilities, decreased employee morale, and productivity

RiskDescription: Failure to identify and address potential hazards and risks faced by women working n

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular safety audits and inspections", "2": "Provide safety training to employees

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 111:

RiskId: 2833

ComplianceId: 3270

RiskTitle: Inadequate Safety Equipment

Criticality: Medium

PossibleDamage: Increased vulnerability to workplace hazards

Category: Operational
RiskType: Current
BusinessImpact: Potential injuries, decreased employee morale, and legal liabilities
RiskDescription: Failure to provide essential safety equipment to women working night shifts can expos
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular maintenance and replacement of safety equipment", "2": "Provide training
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 112:
RiskId: 2834
ComplianceId: 3271
RiskTitle: Legal Liabilities due to Lack of Consent
Criticality: High
PossibleDamage: Legal penalties, reputation damage, employee turnover
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential lawsuits, fines, and negative publicity
RiskDescription: Failure to obtain written consent from women workers for night shifts may result in leg
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide legal guidance on consent requirements", "2": "Implement regular audits
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 113:
RiskId: 2835
ComplianceId: 3272
RiskTitle: Miscommunication in Consent Management
Criticality: Medium
PossibleDamage: Employee grievances, legal disputes, reputation damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Employee dissatisfaction, legal liabilities
RiskDescription: Inadequate training on consent management may result in miscommunication, incorre
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update training modules based on feedback", "2": "Provide refresher co
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 114:
RiskId: 2836
ComplianceId: 3273
RiskTitle: Mismanagement of Social Security Fund
Criticality: High
PossibleDamage: Financial loss, lack of support for unorganized workers
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption in social security benefits, loss of trust in government initiatives
RiskDescription: Inadequate allocation or misuse of funds leading to insufficient support for unorganize

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear fund management guidelines", "2": "Regular independent audits of
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 115:
RiskId: 2837
ComplianceId: 3274
RiskTitle: Failure to Establish Minimum Wage Standards
Criticality: High
PossibleDamage: Exploitation of unorganized workers and legal actions
Category: Operational
RiskType: Current
BusinessImpact: Reputational damage and legal consequences
RiskDescription: Failure to establish minimum wage standards within the specified timeframe may lead
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting of progress in setting wage levels", "2": "Engage
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 116:
RiskId: 2838

ComplianceId: 3275
RiskTitle: Inaccurate Assessment of Regional Economic Conditions
Criticality: Medium
PossibleDamage: Unfair wage levels and dissatisfaction among unorganized workers
Category: Operational
RiskType: Current
BusinessImpact: Challenges in maintaining consistency and fairness in wage levels
RiskDescription: Incorrect assessment of regional economic conditions may result in setting inappropri
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Utilization of economic experts for accurate assessment", "2": "Regular review an
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 117:
RiskId: 2839
ComplianceId: 3276
RiskTitle: Non-compliance with Minimum Wage Standards
Criticality: High
PossibleDamage: Legal penalties, reputation damage, and employee dissatisfaction
Category: Operational
RiskType: Current
BusinessImpact: Underpayment of employees, legal disputes, and negative impact on employer-emplo
RiskDescription: Failure to conduct regular wage reviews may result in non-compliance with minimum
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update payroll systems with minimum wage standards", "2": "Provide tr

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 118:

RiskId: 2840

ComplianceId: 3277

RiskTitle: Inaccurate Leave Balances Tracking

Criticality: High

PossibleDamage: Inaccurate tracking of leave balances leading to potential leave disputes and employ

Category: Operational

RiskType: Residual

BusinessImpact: All departments would be impacted by potential leave disputes and workload disrupti

RiskDescription: Failure to accurately track employee leave balances could result in disputes, decreas

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits of leave balances to ensure accuracy", "2": "Provide training to HR

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 119:

RiskId: 2841

ComplianceId: 3278

RiskTitle: Delayed Leave Request Processing

Criticality: Medium

PossibleDamage: Delayed processing of leave requests leading to employee dissatisfaction and poten

Category: Operational
RiskType: Residual
BusinessImpact: All departments would be impacted by potential staffing issues and decreased morale
RiskDescription: Failure to process leave requests in a timely manner could result in employee dissatis
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated reminders for pending leave requests", "2": "Establish clear
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 120:
RiskId: 2842
ComplianceId: 3279
RiskTitle: Workplace Safety Training Non-Compliance
Criticality: High
PossibleDamage: Increased workplace accidents, injuries, and regulatory fines.
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to conduct annual safety training may lead to employees not being adequately
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training completion", "2": "Provide refresher training session
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 121:
RiskId: 2843
ComplianceId: 3280
RiskTitle: Inadequate Emergency Response Plans
Criticality: High
PossibleDamage: Confusion and delays during emergencies, potential injuries or loss of life
Category: Operational
RiskType: Inherent
BusinessImpact: Delays in response, potential injuries, loss of life
RiskDescription: Failure to have effective emergency response plans in place can lead to confusion, de
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on emergency procedures", "2": "Mock drills to test the
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 122:
RiskId: 2844
ComplianceId: 3281
RiskTitle: Outdated Minimum Wage Levels
Criticality: High
PossibleDamage: Employee dissatisfaction, labor disputes, strikes
Category: Operational
RiskType: Inherent
BusinessImpact: Potential impact on workforce productivity and industrial relations
RiskDescription: Failure to conduct regular wage surveys may result in setting minimum wage levels th

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear timeline and process for conducting wage surveys", "2": "Engage
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 123:
RiskId: 2845
ComplianceId: 3282
RiskTitle: Penalties for Late Payment
Criticality: High
PossibleDamage: Financial penalties, legal actions
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to pay wages on time may result in financial penalties and legal actions agains
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated payroll systems with payment reminders", "2": "Regularly m
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 124:
RiskId: 2846

ComplianceId: 3283
RiskTitle: Payment Processing Errors
Criticality: Medium
PossibleDamage: Incorrect payments, employee dissatisfaction
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Errors in payment processing due to inadequate payroll systems may result in incorre
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Conduct regular audits of payroll systems", "2": "Provide training to employees on
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 125:
RiskId: 2847
ComplianceId: 3284
RiskTitle: Non-Compliance with Social Security Contribution Requirements
Criticality: High
PossibleDamage: Legal penalties, fines, and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Legal actions, financial losses, and damaged reputation
RiskDescription: Failure to comply with social security contribution requirements may lead to legal pena
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits to verify compliance", "2": "Training for finance departments on co

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 126:

RiskId: 2848

ComplianceId: 3285

RiskTitle: Legal Penalties for Non-Compliance

Criticality: High

PossibleDamage: Legal penalties and fines for the organization

Category: Compliance

RiskType: Current

BusinessImpact: Financial loss and damage to the organization's reputation

RiskDescription: Failure to register employees on time may lead to violations of social security regulati

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits to ensure compliance", "2": "Training on registration procedures", "

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 127:

RiskId: 2849

ComplianceId: 3286

RiskTitle: Incorrect Benefits Due to Unreported Changes

Criticality: Medium

PossibleDamage: Incorrect benefits for employees and legal consequences for the organization

Category: Compliance
RiskType: Current
BusinessImpact: Financial loss and damage to the organization's reputation
RiskDescription: Failure to report changes in employment status may lead to incorrect benefits for emp
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting procedures", "2": "Training on reporting requirements", "3
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 128:
RiskId: 2850
ComplianceId: 3287
RiskTitle: Unidentified Workplace Hazards
Criticality: High
PossibleDamage: Potential workplace accidents, injuries, and legal liabilities.
Category: Operational
RiskType: Inherent
BusinessImpact: Workplace productivity may decrease due to accidents and injuries.
RiskDescription: Failure to conduct annual risk assessments may result in unidentified workplace haza
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training on risk assessment procedures", "2": "Utilize external c
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 129:
RiskId: 2851
ComplianceId: 3288
RiskTitle: Workplace Accidents and Injuries
Criticality: High
PossibleDamage: Increased likelihood of workplace accidents and injuries.
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of productivity, increased medical costs, and damage to company repu
RiskDescription: Failure to provide safety equipment and training could result in workplace accidents a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular safety training sessions", "2": "Maintain up-to-date inventory of safety equ
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 130:
RiskId: 2852
ComplianceId: 3289
RiskTitle: Delay in Grievance Resolution for Migrant Workers
Criticality: High
PossibleDamage: Decreased trust and satisfaction among migrant workers
Category: Operational
RiskType: Residual
BusinessImpact: Potential increase in complaints and unrest among migrant workers
RiskDescription: Failure to address grievances in a timely manner can lead to dissatisfaction and poten

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely response to all complaints received through the helpline", "2": "Reg
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 131:
RiskId: 2853
ComplianceId: 3290
RiskTitle: Data Security Breaches on Web-Based Platform
Criticality: Medium
PossibleDamage: Compromised complaint information and potential legal implications
Category: IT
RiskType: Residual
BusinessImpact: Loss of trust and credibility due to data breaches
RiskDescription: Failure to secure the web-based platform used for logging complaints can result in da
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement multi-factor authentication for platform access", "2": "Regularly train st
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 132:
RiskId: 2854

ComplianceId: 3291
RiskTitle: Data Security Breach
Criticality: High
PossibleDamage: Unauthorized access to sensitive worker information
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of trust from migrant workers and potential legal implications
RiskDescription: Unauthorized access to the database can lead to leakage of personal information and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for database access", "2": "Regular security
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 133:
RiskId: 2855
ComplianceId: 3292
RiskTitle: Data Breach in Online System
Criticality: Medium
PossibleDamage: Unauthorized access to worker data
Category: IT
RiskType: Inherent
BusinessImpact: Loss of trust from workers and regulatory fines
RiskDescription: A data breach in the online registration system can lead to exposure of sensitive work
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regular security updates and patches for the system", "2": "Implement intrusion d

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 134:

RiskId: 2856

ComplianceId: 3293

RiskTitle: Risk of Inadequate Night Shift Safety Measures

Criticality: High

PossibleDamage: Increased risk of accidents, injuries, or harm to women workers during night shifts

Category: Operational

RiskType: Inherent

BusinessImpact: All business units employing women workers during night hours

RiskDescription: Failure to implement adequate safety measures for women working night shifts may r

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement regular safety audits and address any identified issues promptly", "2":

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 135:

RiskId: 2857

ComplianceId: 3294

RiskTitle: Violation of Consent Rights

Criticality: High

PossibleDamage: Legal implications and reputational damage

Category: Compliance
RiskType: Inherent
BusinessImpact: Potential lawsuits, fines, and damage to company reputation
RiskDescription: Failure to obtain proper consent from women workers for night shifts may lead to lega
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training to HR staff on consent laws and processes", "2": "Regularly revie
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 136:
RiskId: 2858
ComplianceId: 3295
RiskTitle: Loss of Consent Documentation
Criticality: Medium
PossibleDamage: Inability to prove consent and legal consequences
Category: Compliance
RiskType: Inherent
BusinessImpact: Legal disputes, regulatory fines, and reputational damage
RiskDescription: Failure to manage and maintain consent documentation may result in the inability to p
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a secure document management system with access controls", "2": "R
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 137:
RiskId: 2859
ComplianceId: 3296
RiskTitle: Delay in Fund Establishment
Criticality: High
PossibleDamage: Financial insecurity and lack of social protection for unorganized workers
Category: Operational
RiskType: Inherent
BusinessImpact: Financial instability, social unrest
RiskDescription: Failure to establish the fund within the specified timeframe may result in unorganized
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Allocate dedicated resources for fund establishment", "2": "Regularly monitor prog
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 138:
RiskId: 2860
ComplianceId: 3297
RiskTitle: Inequitable Contribution and Benefits Framework
Criticality: Medium
PossibleDamage: Worker dissatisfaction and financial strain on the fund
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of worker trust, financial instability
RiskDescription: A poorly designed contribution and benefits framework may result in some workers re

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Engage with workers to understand their needs and preferences", "2": "Regularly
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 139:
RiskId: 2861
ComplianceId: 3298
RiskTitle: Technical Issues with Mobile Application
Criticality: High
PossibleDamage: Delayed enrollment and dissatisfaction among unorganized workers
Category: Operational
RiskType: Current
BusinessImpact: Reduced efficiency in enrolling workers and potential reputational damage
RiskDescription: The mobile application may face technical glitches or downtime, impacting the registra
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular maintenance and updates of the application", "2": "24/7 technical support
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 140:
RiskId: 2862

ComplianceId: 3299
RiskTitle: Low Attendance at Outreach Programs
Criticality: Medium
PossibleDamage: Limited reach to unorganized workers and reduced enrollment numbers
Category: Operational
RiskType: Current
BusinessImpact: Decreased program effectiveness and potential resource wastage
RiskDescription: Low attendance at outreach programs may result in reduced awareness and enrollme
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Targeted marketing strategies for program promotion", "2": "Engage local influenc
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 141:
RiskId: 2863
ComplianceId: 3300
RiskTitle: Non-Compliance with Minimum Wage Laws
Criticality: High
PossibleDamage: Potential fines and legal consequences
Category: Compliance
RiskType: Current
BusinessImpact: Legal actions, financial penalties, and reputational damage
RiskDescription: Failure to comply with minimum wage laws could result in legal actions, financial pena
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training for HR staff on minimum wage laws", "2": "Implement automated
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 142:
RiskId: 2864
ComplianceId: 3301
RiskTitle: Inaccurate Leave Balances
Criticality: High
PossibleDamage: Inaccurate leave balances leading to potential employee disputes or compliance viol
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to update leave balances in real-time may result in employees taking more lea
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of leave balances to identify discrepancies", "2": "Employee trainin
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 143:
RiskId: 2865
ComplianceId: 3302
RiskTitle: Lack of HR Oversight
Criticality: Medium
PossibleDamage: Lack of oversight leading to non-compliance with regulatory requirements

Category: Legal
RiskType: Inherent
BusinessImpact: HR department
RiskDescription: Failure of the HR department to oversee leave entitlements could result in violations o
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training for HR staff on leave management policies and procedures", "2":
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 144:
RiskId: 2866
ComplianceId: 3303
RiskTitle: Workplace Accident Risk
Criticality: High
PossibleDamage: Increased workplace accidents and potential legal liabilities
Category: Operational
RiskType: Inherent
BusinessImpact: Increased absenteeism, decreased productivity, potential legal costs
RiskDescription: Lack of safety training may result in employees not following proper safety procedures
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular bi-annual safety training sessions", "2": "Implement safety audits to ensu
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 145:
RiskId: 2867
ComplianceId: 3304
RiskTitle: Delayed Incident Reporting
Criticality: High
PossibleDamage: Delayed incident response may lead to increased severity of incidents, legal liabilitie
Category: Operational
RiskType: Inherent
BusinessImpact: Potential legal consequences, reputational damage, and operational disruptions.
RiskDescription: Failure to report incidents promptly may result in delayed response, inability to addres
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide regular training to employees on incident reporting procedures", "2": "Imp
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 146:
RiskId: 2868
ComplianceId: 3305
RiskTitle: Unidentified Safety Hazards
Criticality: High
PossibleDamage: Workplace accidents, injuries, legal liabilities, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential disruption to operations, increased costs due to accidents, and damage to c
RiskDescription: Failure to identify safety hazards through audits may result in workplace accidents, inj

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust audit checklist to ensure comprehensive coverage of safety s
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 147:
RiskId: 2869
ComplianceId: 3306
RiskTitle: Delayed Reporting of Safety Hazards
Criticality: Medium
PossibleDamage: Workplace accidents, injuries, legal liabilities
Category: Operational
RiskType: Current
BusinessImpact: Increased risk exposure, potential legal consequences, and impact on employee safe
RiskDescription: Delayed reporting of safety hazards may lead to accidents, injuries, and legal liabilitie
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a clear reporting protocol for all employees to follow", "2": "Provide train
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 148:
RiskId: 2870

ComplianceId: 3307
RiskTitle: Lack of Mental Health Training Programs
Criticality: High
PossibleDamage: Increased stress levels, decreased mental well-being, potential mental health crises
Category: Operational
RiskType: Residual
BusinessImpact: Decreased employee productivity, increased absenteeism, potential legal liabilities
RiskDescription: Failure to provide regular mental health training programs may lead to increased stres
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement mandatory mental health training programs", "2": "Provide access to c
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 149:
RiskId: 2871
ComplianceId: 3308
RiskTitle: Inadequate Employee Feedback on Mental Health Services
Criticality: Medium
PossibleDamage: Inadequate mental health support, decreased employee satisfaction, potential legal
Category: Operational
RiskType: Residual
BusinessImpact: Decreased employee morale, potential legal liabilities, reduced effectiveness of ment
RiskDescription: Lack of employee feedback on mental health services may result in inadequate suppo
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement regular employee feedback surveys", "2": "Provide channels for anony

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 150:

RiskId: 2872

ComplianceId: 3309

RiskTitle: Failure to Report Wage Violations

Criticality: High

PossibleDamage: Legal fines, reputational damage, and employee dissatisfaction

Category: Compliance

RiskType: Current

BusinessImpact: Potential legal costs and damage to company reputation

RiskDescription: If wage violations are not reported promptly, the organization may face legal consequ

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear reporting procedures and channels", "2": "Provide training on reco

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 151:

RiskId: 2873

ComplianceId: 3310

RiskTitle: Non-Compliance with Semi-Annual Checks

Criticality: Medium

PossibleDamage: Penalties for non-compliance and reputational harm

Category: Compliance
RiskType: Current
BusinessImpact: Potential financial penalties and damage to company reputation
RiskDescription: If compliance checks are not conducted as required, the organization may face penal
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear guidelines for compliance checks", "2": "Provide resources for com
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 152:
RiskId: 2874
ComplianceId: 3311
RiskTitle: Gender Pay Gap Risk
Criticality: High
PossibleDamage: Legal penalties, loss of talent, and negative media coverage
Category: Compliance
RiskType: Current
BusinessImpact: Potential lawsuits, decreased employee morale, and damage to company reputation
RiskDescription: Failure to address gender pay gaps through equal pay audits could result in legal con
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits and salary adjustments", "2": "Transparent communication on pay
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 153:
RiskId: 2875
ComplianceId: 3312
RiskTitle: Pay Disparity Risk
Criticality: Medium
PossibleDamage: Employee turnover, decreased morale, and legal challenges
Category: Compliance
RiskType: Current
BusinessImpact: Loss of talent, negative impact on employee engagement, and potential legal conseq
RiskDescription: Failure to ensure consistent salary benchmarking and role assessments may lead to
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular benchmarking updates and adjustments", "2": "Clear criteria for role asse
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 154:
RiskId: 2876
ComplianceId: 3313
RiskTitle: Undetected Health Issues
Criticality: High
PossibleDamage: Undetected health issues may lead to serious health complications for employees
Category: Operational
RiskType: Current
BusinessImpact: Decreased employee productivity, increased healthcare costs
RiskDescription: Failure to conduct annual health check-ups may result in employees developing serio

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular communication and reminders to employees about the importance of hea
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 155:
RiskId: 2877
ComplianceId: 3314
RiskTitle: Inaccurate Health Records
Criticality: Medium
PossibleDamage: Inaccurate health records may lead to incorrect medical treatment for employees
Category: Operational
RiskType: Current
BusinessImpact: Potential medical errors, legal issues
RiskDescription: Failure to maintain accurate health records may result in employees receiving incorre
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing a secure electronic health record system", "2": "Training designated
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 156:
RiskId: 2878

ComplianceId: 3315
RiskTitle: Lack of ESIC Coverage for Hazardous Workers
Criticality: High
PossibleDamage: Workers not covered by social security benefits in case of accidents or injuries
Category: Operational
RiskType: Current
BusinessImpact: Potential legal liabilities, financial losses, and reputational damage
RiskDescription: Failure to register workers with ESIC may result in financial and legal consequences f
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of worker registrations", "2": "Training programs for HR on registra
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 157:
RiskId: 2879
ComplianceId: 3316
RiskTitle: Non-Provision of Travel Allowances
Criticality: High
PossibleDamage: Legal penalties, worker strikes, negative reputation.
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, decreased productivity, legal liabilities.
RiskDescription: Failure to provide travel allowances may result in worker unrest and legal repercussio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits to ensure compliance", "2": "Provide clear guidelines to HR depart

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 158:

RiskId: 2880

ComplianceId: 3317

RiskTitle: Non-Registration for Cess Fund Benefits

Criticality: Medium

PossibleDamage: Loss of benefits, worker grievances, legal penalties.

Category: Operational

RiskType: Current

BusinessImpact: Financial losses, decreased worker morale, legal liabilities.

RiskDescription: Failure to register workers for Cess fund benefits may lead to worker dissatisfaction a

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly update worker information in the national portal", "2": "Provide training t

CreatedAt: 2025-11-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 159:

RiskId: 2881

ComplianceId: 3318

RiskTitle: Inaccurate Database Information

Criticality: High

PossibleDamage: Mismanagement of social security benefits and legal protections for unorganized wo

Category: Operational
RiskType: Current
BusinessImpact: Government agencies and employers may face legal consequences and public backl
RiskDescription: Inaccurate database information can lead to the exclusion of eligible workers from soc
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular data quality checks and updates", "2": "Employee training on accurate da
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 160:
RiskId: 2882
ComplianceId: 3319
RiskTitle: Failure to Report Vacancies
Criticality: High
PossibleDamage: Legal fines, reputational harm, and recruitment challenges
Category: Compliance
RiskType: Current
BusinessImpact: Delayed hiring process, loss of potential talent, and negative employer branding
RiskDescription: Non-compliance with vacancy reporting requirements may lead to legal repercussions
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting guidelines and procedures", "2": "Implement regular mon
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 161:
RiskId: 2883
ComplianceId: 3320
RiskTitle: Failure to process pension benefits for eligible workers
Criticality: High
PossibleDamage: Workers may not receive their entitled pension benefits, leading to dissatisfaction an
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, legal consequences, and potential reputational damage.
RiskDescription: The risk of not processing pension benefits for eligible workers can lead to dissatisfac
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly audit pension benefit processing to ensure all eligible workers receive t
CreatedAt: 2025-11-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 162:
RiskId: 2523
ComplianceId: 3189
RiskTitle: Annual Assessment of Cardholder Data Locationss
Criticality: High
PossibleDamage: Unauthorized access to cardholder data, data breaches, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: Conduct a comprehensive assessment of all systems and processes that handle card

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: None
CreatedAt: 2025-11-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 163:
RiskId: 2344
ComplianceId: 3005
RiskTitle: Inadequate Annual Risk Assessment
Criticality: High
PossibleDamage: Unexpected losses, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face financial losses and regulatory scrutiny.
RiskDescription: Failure to conduct an annual risk assessment may lead to unidentified risks and misal
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on risk assessment procedures", "2": "Utilize external consultants
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 164:
RiskId: 2345

ComplianceId: 3006
RiskTitle: Failure to Conduct Ad-hoc Risk Assessment
Criticality: Medium
PossibleDamage: Financial losses, non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: Risk Management and Compliance Departments may face financial losses and regula
RiskDescription: Neglecting ad-hoc risk assessments for significant changes may result in inadequate
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a clear process for identifying and assessing significant changes", "2": "
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 165:
RiskId: 2346
ComplianceId: 3007
RiskTitle: Failure to Verify Customer Identity
Criticality: High
PossibleDamage: Financial loss, regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of business operations, legal consequences, loss of customer trust
RiskDescription: Failure to verify customer identity increases the risk of fraudulent activities and money
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement robust identity verification processes", "2": "Provide regular training on

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 166:

RiskId: 2347

ComplianceId: 3008

RiskTitle: Failure to Adjust Monitoring Parameters

Criticality: Medium

PossibleDamage: Regulatory non-compliance, financial loss, reputational harm

Category: Operational

RiskType: Inherent

BusinessImpact: Increased risk of money laundering, fraud, and regulatory violations

RiskDescription: Failure to adjust monitoring parameters for high-risk customers may result in undetect

RiskLikelihood: 6

RiskImpact: 8

RiskExposureRating: 48

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly review and update monitoring parameters based on risk assessments",

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 167:

RiskId: 2348

ComplianceId: 3009

RiskTitle: Inaccurate Wealth Source Disclosure

Criticality: High

PossibleDamage: Increased risk of money laundering, fraud, and regulatory penalties

Category: Compliance
RiskType: Current
BusinessImpact: Legal and regulatory non-compliance, financial losses, reputational damage
RiskDescription: Failure to verify client wealth sources accurately may lead to potential illegal activities
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance client due diligence procedures", "2": "Implement automated verification
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 168:
RiskId: 2349
ComplianceId: 3010
RiskTitle: Outdated Wealth Source Information
Criticality: Medium
PossibleDamage: Increased risk of using inaccurate client wealth sources for transactions
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, compliance breaches
RiskDescription: Failure to review and update client wealth sources annually may lead to using outdate
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate annual review processes", "2": "Enhance data validation checks for wea
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 169:
RiskId: 2350
ComplianceId: 3011
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, and legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties, and regulatory scrutiny
RiskDescription: Failure to detect suspicious activities through transaction monitoring may lead to seve
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced transaction monitoring system", "2": "Regular staff training on detecting
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 170:
RiskId: 2351
ComplianceId: 3012
RiskTitle: Outdated Client Information
Criticality: Medium
PossibleDamage: Regulatory fines, increased risk exposure, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate risk assessments, regulatory scrutiny, and potential legal consequences
RiskDescription: Failure to update client information may result in inaccurate risk assessments and nor

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated data validation processes", "2": "Client outreach for information update
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 171:
RiskId: 2352
ComplianceId: 3013
RiskTitle: Inadequate Client Risk Assessment Documentation
Criticality: High
PossibleDamage: Increased exposure to financial crimes and regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, loss of reputation, and client trust
RiskDescription: Failure to document risk assessments may result in incomplete due diligence, leading
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation requirements", "2": "Automated documentation
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 172:
RiskId: 2353

ComplianceId: 3014
RiskTitle: Inadequate Ongoing Monitoring of Client Transactions
Criticality: Medium
PossibleDamage: Undetected financial crimes and regulatory violations
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, loss of reputation, and legal consequences
RiskDescription: Failure to monitor client transactions may lead to undetected money laundering or oth
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated transaction monitoring systems", "2": "Regular training on transaction
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 173:
RiskId: 2354
ComplianceId: 3015
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Non-compliance penalties, loss of client trust, financial losses
RiskDescription: Undetected suspicious activities may result in regulatory violations and reputational da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update PEP and sanctions lists for accurate screening", "2": "Conduct p

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 174:

RiskId: 2355

ComplianceId: 3016

RiskTitle: Undetected Anomalies in Transaction Patterns

Criticality: Medium

PossibleDamage: Regulatory non-compliance, financial losses

Category: Operational

RiskType: Current

BusinessImpact: Non-compliance penalties, financial losses

RiskDescription: Failure to detect anomalies in transaction patterns may lead to undetected suspicious

RiskLikelihood: 6

RiskImpact: 8

RiskExposureRating: 48

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear criteria for identifying anomalies in transaction patterns", "2": "Impl

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 175:

RiskId: 2356

ComplianceId: 3017

RiskTitle: Failure to Obtain Senior Management Approval for PEP Relationships

Criticality: High

PossibleDamage: Reputational damage, regulatory fines, and financial losses.

Category: Compliance
RiskType: Inherent
BusinessImpact: Disruption of operations, loss of client trust, and legal consequences.
RiskDescription: Failure to obtain senior management approval for PEP relationships can result in inac
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear approval criteria and documentation requirements", "2": "Provide r
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 176:
RiskId: 2357
ComplianceId: 3018
RiskTitle: Client Risk Exposure
Criticality: High
PossibleDamage: Financial losses, reputational damage, and regulatory penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Significant financial impact and reputational damage
RiskDescription: Failure to assess client risk factors adequately may result in exposure to high-risk clie
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence processes for high-risk clients", "2": "Implement transactio
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 177:
RiskId: 2358
ComplianceId: 3019
RiskTitle: Inadequate Training on EDD Practices
Criticality: High
PossibleDamage: Increased risk of staff failing to identify and report suspicious activities, leading to po
Category: Operational
RiskType: Inherent
BusinessImpact: Potential regulatory fines, reputational damage, and legal implications.
RiskDescription: Failure to adequately train staff on EDD practices may result in missed red flags for m
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update training materials to reflect current EDD practices and complian
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 178:
RiskId: 2359
ComplianceId: 3020
RiskTitle: Undetected Financial Crime Risks
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Significant impact on compliance, financial stability, and reputation
RiskDescription: Failure to monitor transactions in real-time may lead to undetected financial crime risk

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance transaction monitoring systems", "2": "Regularly update red flag indicato
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 179:
RiskId: 2360
ComplianceId: 3021
RiskTitle: Delayed Detection of Financial Crime Risks
Criticality: Medium
PossibleDamage: Financial losses, regulatory scrutiny, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Negative impact on compliance effectiveness and reputation
RiskDescription: Failure to conduct quarterly reviews may lead to delayed detection of financial crime r
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear review timelines", "2": "Enhance review quality through training", "
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 180:
RiskId: 2361

ComplianceId: 3022
RiskTitle: Risk of Non-Compliance with High-Risk Customer Assessments
Criticality: High
PossibleDamage: Legal actions, financial penalties, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Legal consequences, financial losses, reputational damage
RiskDescription: Failure to conduct comprehensive risk assessments for high-risk customers may expo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures for high-risk customers", "2": "Regularly updat
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 181:
RiskId: 2362
ComplianceId: 3023
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Increased compliance risks, regulatory scrutiny, financial penalties
RiskDescription: The inability to detect suspicious activities in real-time may result in severe financial a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhance transaction monitoring algorithms for better detection accuracy", "2": "Re

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 182:

RiskId: 2363

ComplianceId: 3024

RiskTitle: Missed Suspicious Activities During Monthly Reviews

Criticality: Medium

PossibleDamage: Regulatory penalties, reputational damage

Category: Operational

RiskType: Inherent

BusinessImpact: Increased compliance risks, regulatory scrutiny

RiskDescription: Failure to conduct thorough monthly reviews may result in regulatory violations and re

RiskLikelihood: 6

RiskImpact: 8

RiskExposureRating: 48

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Automate review processes to reduce manual errors", "2": "Implement peer reviev

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 183:

RiskId: 2364

ComplianceId: 3025

RiskTitle: Inadequate Staff Training

Criticality: High

PossibleDamage: Potential regulatory violations, financial losses, and reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Human Resources, Compliance Departments
RiskDescription: Failure to provide adequate training may result in staff not being able to effectively ide
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training updates based on regulatory changes", "2": "Implement knowled
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 184:
RiskId: 2365
ComplianceId: 3026
RiskTitle: Failure to Conduct Annual Risk Assessment
Criticality: High
PossibleDamage: Accepting risks beyond tolerance level
Category: Operational
RiskType: Current
BusinessImpact: All business units impacted by unidentified risks
RiskDescription: Failure to conduct annual risk assessment may result in inadequate risk management
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Utilize risk assessment frameworks and tools", "2": "Document findings accurately
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 185:
RiskId: 2366
ComplianceId: 3027
RiskTitle: Undefined Risk Appetite Statement
Criticality: Medium
PossibleDamage: Strategic misalignment and increased risk exposure
Category: Strategic
RiskType: Current
BusinessImpact: Compromised strategic objectives
RiskDescription: Undefined risk appetite statement may lead to inconsistent risk management decision
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Involve key stakeholders in defining risk appetite", "2": "Regularly review and upd
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 186:
RiskId: 2367
ComplianceId: 3028
RiskTitle: Inaccurate Customer Occupation Information
Criticality: High
PossibleDamage: Increased exposure to financial crimes
Category: Operational
RiskType: Inherent
BusinessImpact: Potential regulatory fines and reputational damage
RiskDescription: Failure to verify customer occupation accurately may lead to increased risk of financia

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify occupation through official documents", "2": "Conduct periodic reviews of cu
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 187:
RiskId: 2368
ComplianceId: 3029
RiskTitle: Outdated Customer Information
Criticality: Medium
PossibleDamage: Increased risk exposure
Category: Operational
RiskType: Inherent
BusinessImpact: Inaccurate risk assessment and potential regulatory non-compliance
RiskDescription: Failure to update customer information regularly may result in outdated risk assessme
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated alerts for information updates", "2": "Conduct periodic revie
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 188:
RiskId: 2369

ComplianceId: 3030
RiskTitle: Undetected Suspicious Transactions
Criticality: High
PossibleDamage: Financial losses, regulatory penalties, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Failure to detect suspicious transactions can result in severe financial and reputationa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring systems", "2": "Conduct regular manual reviews
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 189:
RiskId: 2370
ComplianceId: 3031
RiskTitle: Insufficient Transaction Monitoring Intensity
Criticality: Medium
PossibleDamage: Financial losses, regulatory penalties
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory fines
RiskDescription: Inadequate scrutiny of transaction patterns and anomalies can result in missed suspic
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement advanced analytics tools", "2": "Conduct in-depth manual reviews", "3"

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 190:

RiskId: 2371

ComplianceId: 3032

RiskTitle: Inaccurate Client Net Worth Assessment

Criticality: High

PossibleDamage: Improper risk assessment and potential regulatory non-compliance

Category: Operational

RiskType: Current

BusinessImpact: May lead to financial losses or reputational damage

RiskDescription: Failure to accurately assess a client's total net worth may result in improper risk mana

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training for staff on proper documentation requirements", "2": "Automated

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 191:

RiskId: 2372

ComplianceId: 3033

RiskTitle: Unverified Source of Wealth Information

Criticality: Medium

PossibleDamage: Exposure to financial crimes and regulatory scrutiny

Category: Operational
RiskType: Current
BusinessImpact: May lead to legal penalties or reputational damage
RiskDescription: Failure to verify the source of wealth information provided by clients may expose the c
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear procedures for public source verification", "2": "Implement automat
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 192:
RiskId: 2373
ComplianceId: 3034
RiskTitle: Inaccurate Client Document Verification
Criticality: High
PossibleDamage: Risk of financial fraud and money laundering
Category: Compliance
RiskType: Current
BusinessImpact: Potential regulatory fines, reputational damage, and legal consequences
RiskDescription: Failure to accurately verify client-provided documents may result in facilitating financia
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated document verification tools", "2": "Conduct periodic audits c
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 193:
RiskId: 2374
ComplianceId: 3035
RiskTitle: Outdated Source of Wealth Information
Criticality: Medium
PossibleDamage: Risk of financial non-compliance and exposure to illicit activities
Category: Compliance
RiskType: Current
BusinessImpact: Potential regulatory scrutiny, financial penalties, and reputational damage
RiskDescription: Failure to periodically verify source of wealth information may result in outdated or ina
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate periodic source of wealth verification processes", "2": "Implement alerts
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 194:
RiskId: 2375
ComplianceId: 3036
RiskTitle: Inaccurate High-Risk Customer Assessment
Criticality: High
PossibleDamage: Potential money laundering, fraud, or reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Regulatory fines, loss of reputation, legal action
RiskDescription: Failure to accurately assess high-risk customers may result in the facilitation of illicit a

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement enhanced due diligence procedures for high-risk customers", "2": "Pro
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 195:
RiskId: 2376
ComplianceId: 3037
RiskTitle: Undetected Changes in High-Risk Customer Risk Profile
Criticality: High
PossibleDamage: Potential money laundering, fraud, or reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Regulatory fines, loss of reputation, legal action
RiskDescription: Failure to review high-risk customers annually may result in undetected changes in ris
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated alerts for significant changes in customer risk profiles", "2":
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 196:
RiskId: 2377

ComplianceId: 3038
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial integrity and regulatory compliance
RiskDescription: Failure to detect and report suspicious activities can result in severe financial and rep
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for transaction monitoring team on identifying suspicious activitie
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 197:
RiskId: 2378
ComplianceId: 3039
RiskTitle: Non-compliance with EDD Processes
Criticality: High
PossibleDamage: Regulatory fines, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Compliance, Legal
RiskDescription: Failure to comply with EDD processes can result in regulatory penalties and reputatio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training sessions", "2": "Online modules for remote staff", "3": "Knowledg

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 198:

RiskId: 2379

ComplianceId: 3040

RiskTitle: Failure to Verify Customer Identity

Criticality: High

PossibleDamage: Money laundering, fraud, regulatory fines

Category: Compliance

RiskType: Inherent

BusinessImpact: Legal and financial consequences

RiskDescription: Failure to verify customer identity may result in facilitating illicit activities through the b

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhance customer due diligence procedures", "2": "Implement automated verifica

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 199:

RiskId: 2380

ComplianceId: 3041

RiskTitle: Outdated Customer Identification Information

Criticality: Medium

PossibleDamage: Increased risk of money laundering and fraud

Category: Compliance
RiskType: Inherent
BusinessImpact: Legal and financial consequences
RiskDescription: Outdated customer identification information may result in the inability to detect suspic
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated monitoring tools for identification updates", "2": "Enhance c
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 200:
RiskId: 2381
ComplianceId: 3042
RiskTitle: Undetected Fraudulent Transactions
Criticality: High
PossibleDamage: Financial loss due to fraudulent activities
Category: Operational
RiskType: Inherent
BusinessImpact: Risk Management Team
RiskDescription: Failure to detect suspicious activities in customer transactions can result in financial lo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular system updates and maintenance", "2": "Continuous staff training on syst
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 201:
RiskId: 2382
ComplianceId: 3043
RiskTitle: Delayed Detection of Fraudulent Transactions
Criticality: Medium
PossibleDamage: Financial loss due to delayed detection of fraudulent activities
Category: Operational
RiskType: Inherent
BusinessImpact: Compliance Staff
RiskDescription: If transactions are not monitored in real-time, there is a risk of delayed detection of fra
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated alerts for real-time monitoring", "2": "Regular training for compliance s
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 202:
RiskId: 2383
ComplianceId: 3044
RiskTitle: Undisclosed Ownership Risk
Criticality: High
PossibleDamage: Involvement in illicit activities or money laundering
Category: Compliance
RiskType: Current
BusinessImpact: Compliance Department
RiskDescription: Failure to assess ownership structure may result in the institution unknowingly facilita

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence procedures", "2": "Regular training for compliance officer
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 203:
RiskId: 2384
ComplianceId: 3045
RiskTitle: Missed Ownership Changes Risk
Criticality: Medium
PossibleDamage: Missed red flags or changes in customer behavior
Category: Compliance
RiskType: Current
BusinessImpact: Compliance Department
RiskDescription: Failure to review ownership structures may lead to delayed detection of suspicious ac
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated monitoring systems for ownership changes", "2": "Regular training for
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 204:
RiskId: 2385

ComplianceId: 3046
RiskTitle: Undetected Customer Risks
Criticality: High
PossibleDamage: Financial losses due to fraudulent activities or regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of revenue, damage to reputation, legal consequences
RiskDescription: Failure to identify and mitigate customer risks can lead to financial fraud, money laund
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance customer due diligence processes", "2": "Implement transaction monitor
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 205:
RiskId: 2386
ComplianceId: 3047
RiskTitle: Inadequate Staff Training
Criticality: High
PossibleDamage: Errors in EDD processes, potential regulatory violations, and reputational damage.
Category: Operational
RiskType: Residual
BusinessImpact: Disruption to EDD processes, regulatory fines, and reputational harm.
RiskDescription: Lack of adequate training may result in staff errors in EDD processes, leading to regu
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly update training materials to reflect current regulations and best practice
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 206:
RiskId: 2387
ComplianceId: 3048
RiskTitle: Inadequate Documentation of Customer Profiles
Criticality: High
PossibleDamage: Inadequate risk assessments and potential non-compliance with regulations
Category: Compliance
RiskType: Residual
BusinessImpact: Compromised customer due diligence processes and regulatory compliance
RiskDescription: Failure to document customer profiles accurately may lead to inadequate risk assessr
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement training programs for staff on proper documentation procedures", "2": "
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 207:
RiskId: 2388
ComplianceId: 3049
RiskTitle: Inadequate Security of Document Management Systems
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive customer information and potential data breaches

Category: IT
RiskType: Residual
BusinessImpact: Compromised data security and regulatory compliance
RiskDescription: Inadequate security measures may result in unauthorized access to sensitive custom
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement encryption and access controls on document management systems", "
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 208:
RiskId: 2389
ComplianceId: 3050
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Potential regulatory fines, loss of reputation, financial penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Non-compliance with EDD requirements, financial losses, reputational damage
RiskDescription: Failure to detect suspicious activities for higher-risk customers due to inadequate mon
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and test the monitoring systems to ensure accuracy", "2": "Prov
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 209:
RiskId: 2390
ComplianceId: 3051
RiskTitle: Failure to Conduct Quarterly Manual Reviews
Criticality: Medium
PossibleDamage: Potential regulatory scrutiny, non-compliance penalties, reputational harm
Category: Operational
RiskType: Inherent
BusinessImpact: Non-compliance with EDD requirements, regulatory fines, reputational damage
RiskDescription: Failure to conduct quarterly manual reviews of high-risk customer transactions may le
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear review procedures and documentation requirements", "2": "Provid
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 210:
RiskId: 2391
ComplianceId: 3052
RiskTitle: Unresolved Audit Findings
Criticality: High
PossibleDamage: Potential regulatory fines, reputational damage, and increased operational risks
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption to operations, financial losses, and reputational harm
RiskDescription: Failure to address audit findings in a timely manner may result in non-compliance with

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear accountability for remediation actions", "2": "Regularly monitor pro
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 211:
RiskId: 2392
ComplianceId: 3053
RiskTitle: Delayed Remediation Actions
Criticality: Medium
PossibleDamage: Prolonged exposure to identified risks, compliance violations, and operational disrup
Category: Operational
RiskType: Residual
BusinessImpact: Increased regulatory scrutiny, potential fines, and operational inefficiencies
RiskDescription: Failure to initiate remediation actions within the specified timeline may result in ongoi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish automated reminders for action initiation deadlines", "2": "Conduct regul
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 212:
RiskId: 2393

ComplianceId: 3054
RiskTitle: Financial Crime Risk from High-Risk Customers
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory penalties, legal actions, and reputational harm
RiskDescription: High-risk customers pose a significant threat of engaging in illicit financial activities, n
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence procedures", "2": "Regular updates to risk assessment to
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 213:
RiskId: 2394
ComplianceId: 3055
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to detect suspicious activities can lead to financial losses and regulatory non-c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Enhanced training for monitoring teams", "2": "Regular system updates for monito
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 214:
RiskId: 2395
ComplianceId: 3056
RiskTitle: Undetected ML/TF Risks
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Regulatory sanctions, financial losses, reputational damage
RiskDescription: Failure to identify and assess ML/TF risks may lead to non-compliance with regulation
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance training on risk identification and assessment", "2": "Implement automat
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 215:
RiskId: 2396
ComplianceId: 3057
RiskTitle: Lack of Approved Risk Appetite Statement
Criticality: High
PossibleDamage: Unclear risk tolerance levels and inconsistent risk management practices

Category: Operational
RiskType: Inherent
BusinessImpact: Executive decision-making, strategic planning, risk management practices
RiskDescription: The absence of an approved risk appetite statement may lead to ambiguity in risk-tak
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular communication and collaboration between Executive Management Team
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 216:
RiskId: 2397
ComplianceId: 3058
RiskTitle: Inaccurate Client Net Worth Data
Criticality: High
PossibleDamage: Incorrect financial assessments, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Financial decisions based on incorrect data, potential regulatory penalties
RiskDescription: Failure to collect accurate net worth information may lead to incorrect financial assess
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular training for client onboarding team on effective data collection te
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 217:
RiskId: 2398
ComplianceId: 3059
RiskTitle: Money Laundering Risk
Criticality: High
PossibleDamage: Legal penalties, loss of reputation, financial losses
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, loss of credibility, legal actions
RiskDescription: Failure to gather accurate source of wealth information may lead to potential money la
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust interview protocols to ensure thorough information gathering", "
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 218:
RiskId: 2399
ComplianceId: 3060
RiskTitle: Undisclosed Source of Wealth Risk
Criticality: High
PossibleDamage: Potential involvement in money laundering or financial crimes
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, reputational damage, and legal consequences
RiskDescription: Failure to verify the source of wealth may result in the organization unknowingly facilit

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance client due diligence procedures", "2": "Implement enhanced monitoring f
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 219:
RiskId: 2400
ComplianceId: 3061
RiskTitle: Inaccurate Third-Party Verification Risk
Criticality: Medium
PossibleDamage: Misrepresentation of client wealth sources
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased exposure to regulatory scrutiny and potential legal implications
RiskDescription: Relying on inaccurate third-party verification may result in the organization unknowing
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Diversify third-party verification sources", "2": "Establish clear criteria for third-part
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 220:
RiskId: 2401

ComplianceId: 3062
RiskTitle: Failure to Verify Due Diligence Documentation
Criticality: High
PossibleDamage: Potential money laundering activities going undetected
Category: Operational
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial penalties, and reputational damage
RiskDescription: If due diligence documentation is not properly verified, there is a high risk of facilitatin
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated document verification tools", "2": "Provide regular training t
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 221:
RiskId: 2402
ComplianceId: 3063
RiskTitle: Failure to Monitor Client Due Diligence Information
Criticality: Medium
PossibleDamage: Missed red flags for potential money laundering activities
Category: Operational
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny and potential financial penalties
RiskDescription: If client due diligence information is not regularly monitored, there is a medium risk of
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement automated monitoring tools", "2": "Establish clear procedures for upda
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 222:
RiskId: 2403
ComplianceId: 3064
RiskTitle: Inadequate Customer Occupation Information
Criticality: High
PossibleDamage: Inaccurate risk assessment, potential exposure to financial crimes
Category: Compliance
RiskType: Residual
BusinessImpact: Compliance, Financial
RiskDescription: Failure to collect and verify customer occupation information may lead to inadequate
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for compliance officers and customer service representatives on
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 223:
RiskId: 2404
ComplianceId: 3065
RiskTitle: Outdated Customer Source of Wealth Information
Criticality: Medium
PossibleDamage: Inaccurate risk assessment, potential exposure to financial crimes

Category: Compliance
RiskType: Residual
BusinessImpact: Compliance, Financial
RiskDescription: Failure to update customer source of wealth information may result in inadequate risk
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated alerts for significant changes in customer behavior", "2": "C
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 224:
RiskId: 2405
ComplianceId: 3066
RiskTitle: Undetected Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory penalties, reputational damage
RiskDescription: Failure to monitor high-risk customers may result in undetected suspicious activities, l
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated alerts for unusual activities", "2": "Enhance staff training on
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 225:
RiskId: 2406
ComplianceId: 3067
RiskTitle: Misclassification of Customer Risk Levels
Criticality: Medium
PossibleDamage: Compliance breaches, financial losses, regulatory penalties
Category: Operational
RiskType: Current
BusinessImpact: Compliance breaches, financial losses, regulatory penalties
RiskDescription: Failure to adjust customer profiles based on new information may lead to misclassifica
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement regular profile review processes", "2": "Leverage analytics tools for pro
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 226:
RiskId: 2407
ComplianceId: 3068
RiskTitle: Incomplete Customer Identification Information
Criticality: High
PossibleDamage: Identity theft, fraud, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Failure to collect accurate customer identification information may lead to unauthorize

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement staff training on proper identification verification procedures", "2": "Imp
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 227:
RiskId: 2408
ComplianceId: 3069
RiskTitle: Delayed Customer Information Verification
Criticality: Medium
PossibleDamage: Unauthorized account access, fraud, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, reputational damage, regulatory penalties
RiskDescription: Failure to verify customer identification information within the specified timeline may re
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated verification systems for efficiency", "2": "Establish clear ver
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 228:
RiskId: 2409

ComplianceId: 3070
RiskTitle: Undetected Money Laundering Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, and loss of customer trust
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal consequences, and reputational harm
RiskDescription: Failure to detect money laundering activities can result in severe financial and reputat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring systems", "2": "Conduct regular manual reviews
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 229:
RiskId: 2410
ComplianceId: 3071
RiskTitle: Outdated Customer Information
Criticality: Medium
PossibleDamage: Non-compliance penalties and increased risk of financial crimes
Category: Operational
RiskType: Current
BusinessImpact: Financial penalties, reputational damage, and increased regulatory scrutiny
RiskDescription: Failure to maintain accurate customer information can result in penalties for non-comp
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement automated data validation processes", "2": "Require customers to peri
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 230:
RiskId: 2411
ComplianceId: 3072
RiskTitle: Financial Crime Risk
Criticality: High
PossibleDamage: Potential regulatory fines and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial and reputational damage
RiskDescription: Failure to identify PEPs accurately may lead to increased risk exposure to financial cr
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for compliance officers on PEP identification procedures", "2": "In
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 231:
RiskId: 2412
ComplianceId: 3073
RiskTitle: Outdated Risk Profile Risk
Criticality: Medium
PossibleDamage: Increased exposure to financial crimes due to outdated risk profiles

Category: Compliance
RiskType: Inherent
BusinessImpact: Financial and reputational damage
RiskDescription: Failure to review PEP risk assessments may result in outdated risk profiles and increa
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated risk assessment tools", "2": "Establish clear criteria for re-a
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 232:
RiskId: 2413
ComplianceId: 3074
RiskTitle: Undetected Suspicious PEP Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial penalties, loss of trust
RiskDescription: Failure to detect suspicious transactions involving PEPs could result in severe conse
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance transaction monitoring capabilities through technology upgrades", "2": "I
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 233:
RiskId: 2414
ComplianceId: 3075
RiskTitle: Non-Compliance with PEP Screening
Criticality: Medium
PossibleDamage: Exposure to sanctioned individuals, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Legal consequences, reputational damage
RiskDescription: Failure to conduct regular screenings against PEP lists could result in inadvertent dea
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate screening processes for efficiency", "2": "Implement a review process fo
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 234:
RiskId: 2415
ComplianceId: 3076
RiskTitle: Inappropriate Investment Offerings
Criticality: High
PossibleDamage: Financial losses for clients and potential regulatory penalties for the institution
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of client trust, financial implications, regulatory consequences
RiskDescription: The risk of offering unsuitable investment products to clients due to inadequate suitab

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement standardized assessment tools and documentation processes", "2": "P
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 235:
RiskId: 2416
ComplianceId: 3077
RiskTitle: Documentation Deficiency
Criticality: Medium
PossibleDamage: Challenges in justifying suitability assessments to clients and regulators
Category: Operational
RiskType: Inherent
BusinessImpact: Reputational risk, regulatory scrutiny, client dissatisfaction
RiskDescription: The risk of lacking detailed documentation for client suitability assessments, leading t
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a centralized documentation system for all assessments", "2": "Regula
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 236:
RiskId: 2417

ComplianceId: 3078
RiskTitle: Missed Red Flags in High-Value Transactions
Criticality: High
PossibleDamage: Increased risk of money laundering and fraud
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Failure to identify red flags in high-value transactions may lead to potential money lau
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced training on red flag identification", "2": "Regular audits of high-value tra
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 237:
RiskId: 2418
ComplianceId: 3079
RiskTitle: Inadequate Training for New Staff on EDD Principles
Criticality: Medium
PossibleDamage: Increased risk of money laundering and fraud
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Inadequate training for new staff may result in missed red flags in high-value transacti
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Enhanced training programs for new staff", "2": "Regular assessments to measure

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 238:

RiskId: 2419

ComplianceId: 3080

RiskTitle: Failure to Detect Suspicious Activities

Criticality: High

PossibleDamage: Potential money laundering or fraud activities going undetected

Category: Compliance

RiskType: Inherent

BusinessImpact: Impact on regulatory compliance and reputation

RiskDescription: Failure to detect suspicious activities in high-value transactions could lead to severe r

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhanced staff training on transaction monitoring", "2": "Regular system updates

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 239:

RiskId: 2420

ComplianceId: 3081

RiskTitle: Inaccurate Transaction Records

Criticality: Medium

PossibleDamage: Non-compliance with regulatory requirements and inaccurate reporting

Category: Compliance
RiskType: Inherent
BusinessImpact: Impact on regulatory compliance and reporting accuracy
RiskDescription: Inaccurate or incomplete transaction records could lead to regulatory violations and m
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 43.2
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish audit checklist and procedures", "2": "Regular training for audit staff", "3
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 240:
RiskId: 2421
ComplianceId: 3082
RiskTitle: Failure to Verify High-Risk Customers
Criticality: High
PossibleDamage: Potential money laundering activities or financial fraud
Category: Compliance
RiskType: Inherent
BusinessImpact: Legal penalties, reputational damage, financial losses
RiskDescription: Failure to collect comprehensive documentation from high-risk customers may result i
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust customer verification procedures", "2": "Regularly update custo
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 241:
RiskId: 2422
ComplianceId: 3083
RiskTitle: Delayed Verification of High-Risk Customer Documentation
Criticality: Medium
PossibleDamage: Increased risk of financial crimes or regulatory violations
Category: Operational
RiskType: Inherent
BusinessImpact: Legal penalties, regulatory fines
RiskDescription: Failure to verify high-risk customer documentation within the specified timeline may re
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated verification processes", "2": "Establish clear escalation proc
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 242:
RiskId: 2423
ComplianceId: 3084
RiskTitle: Failure to Detect Suspicious Transactions
Criticality: High
PossibleDamage: Financial penalties, reputational damage, regulatory sanctions
Category: Compliance
RiskType: Inherent
BusinessImpact: Non-compliance may lead to severe financial and reputational consequences
RiskDescription: Not detecting suspicious transactions in a timely manner can result in severe legal an

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance staff training on red flag identification", "2": "Regularly update monitoring
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 243:
RiskId: 2424
ComplianceId: 3085
RiskTitle: Delayed Reporting of Suspicious Activities
Criticality: Medium
PossibleDamage: Further criminal activities, regulatory fines, reputational harm
Category: Compliance
RiskType: Inherent
BusinessImpact: Delayed reporting may result in regulatory penalties and reputational damage
RiskDescription: Failing to report suspicious activities promptly can lead to increased risks of money la
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting timelines and procedures", "2": "Implement escalation pr
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 244:
RiskId: 2425

ComplianceId: 3086
RiskTitle: Failure to Verify Beneficial Owners
Criticality: High
PossibleDamage: Financial penalties, reputational damage, legal actions
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, loss of customer trust, legal liabilities
RiskDescription: Failure to verify beneficial owners may lead to involvement in illicit activities, regulator
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance verification processes with advanced technology", "2": "Regular audits o
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 245:
RiskId: 2426
ComplianceId: 3087
RiskTitle: Incomplete Risk Assessment Documentation
Criticality: High
PossibleDamage: Missing critical risks and non-compliance with regulatory requirements
Category: Operational
RiskType: Current
BusinessImpact: Non-compliance penalties, reputational damage
RiskDescription: Failure to review the risk assessment documentation may result in missing critical risk
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Perform regular training for auditors on risk assessment review process", "2": "Imp

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 246:

RiskId: 2427

ComplianceId: 3088

RiskTitle: Ineffective Policy and Procedure Management

Criticality: High

PossibleDamage: Inadequate risk management and potential regulatory violations

Category: Operational

RiskType: Inherent

BusinessImpact: All departments involved in EDD may face operational disruptions and regulatory scru

RiskDescription: Failure to effectively manage policies and procedures may lead to gaps in risk manag

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training sessions for staff on policy and procedure updates", "2": "Implem

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 247:

RiskId: 2428

ComplianceId: 3089

RiskTitle: Staff Training Attendance Risk

Criticality: High

PossibleDamage: Lack of attendance may result in staff not having necessary knowledge and skills for

Category: Operational
RiskType: Current
BusinessImpact: All business units involved in EDD processes
RiskDescription: Failure to ensure staff attendance for training sessions may lead to gaps in knowledge
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reminders and notifications for training sessions", "2": "Provide alternative
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 248:
RiskId: 2429
ComplianceId: 3090
RiskTitle: Knowledge Testing Risk
Criticality: Medium
PossibleDamage: Lack of knowledge may result in staff making errors in EDD processes.
Category: Operational
RiskType: Current
BusinessImpact: All business units involved in EDD processes
RiskDescription: Failure to assess staff knowledge through testing may lead to gaps in understanding
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide additional training for staff who do not pass knowledge tests", "2": "Regul
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 249:
RiskId: 2430
ComplianceId: 3091
RiskTitle: Inaccurate Documentation Risk
Criticality: High
PossibleDamage: Regulatory fines, legal actions, financial loss, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All departments handling customer profiles and transaction records
RiskDescription: Inaccurate documentation may lead to regulatory non-compliance, financial loss, or re
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training on documentation standards", "2": "Implement automa
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 250:
RiskId: 2431
ComplianceId: 3092
RiskTitle: Inaccessible Documentation Risk
Criticality: Medium
PossibleDamage: Operational inefficiencies, compliance issues, decision-making delays
Category: Operational
RiskType: Residual
BusinessImpact: All departments handling customer profiles and transaction records
RiskDescription: Inaccessible documentation may hinder operational efficiency, decision-making, and c

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement secure document management systems", "2": "Enforce access control
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 251:
RiskId: 2432
ComplianceId: 3093
RiskTitle: Ineffective Remediation Action Plan
Criticality: High
PossibleDamage: Increased risk exposure, compliance breaches, financial penalties
Category: Operational
RiskType: Residual
BusinessImpact: Delayed remediation, regulatory non-compliance, reputational harm
RiskDescription: Failure to develop and implement an effective remediation action plan may result in u
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of remediation progress", "2": "Escalation of unresolved issue
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 252:
RiskId: 2433

ComplianceId: 3094
RiskTitle: Incomplete Audit Planning
Criticality: High
PossibleDamage: Incomplete audits, missed objectives, resource inefficiencies
Category: Operational
RiskType: Inherent
BusinessImpact: May lead to regulatory non-compliance, financial losses, and reputational damage.
RiskDescription: Failure to develop a comprehensive audit plan may result in incomplete audits, misse
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of the audit plan", "2": "Training for audit team on plan
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 253:
RiskId: 2434
ComplianceId: 3095
RiskTitle: Non-compliance with Annual EDD Audits
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation, disruptions to operations
RiskDescription: Failure to conduct annual EDD audits may result in non-compliance with regulations,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement automated reminders for annual audits", "2": "Regularly update audit p
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 254:
RiskId: 2435
ComplianceId: 3096
RiskTitle: Inaccurate Audit Reporting
Criticality: High
PossibleDamage: Misinformed decision-making, regulatory non-compliance, financial losses, reputatio
Category: Operational
RiskType: Inherent
BusinessImpact: Direct impact on audit, compliance, and risk management functions
RiskDescription: Failure to accurately document audit findings and recommendations may lead to seric
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a review process for audit reports to ensure accuracy", "2": "Provide tr
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 255:
RiskId: 2436
ComplianceId: 3097
RiskTitle: Delayed Corrective Action Implementation
Criticality: Medium
PossibleDamage: Recurring issues, regulatory non-compliance, financial losses

Category: Operational
RiskType: Inherent
BusinessImpact: Direct impact on compliance and risk management functions
RiskDescription: Failure to track and implement corrective actions in a timely manner may lead to ongo
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear timelines for corrective action implementation", "2": "Regularly mo
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 256:
RiskId: 2437
ComplianceId: 3098
RiskTitle: Failure to Update Risk Profiles
Criticality: High
PossibleDamage: Inadequate risk mitigation strategies and potential financial crimes
Category: Compliance
RiskType: Current
BusinessImpact: Increased exposure to financial crimes and regulatory fines
RiskDescription: Failure to update risk profiles may result in insufficient monitoring of high-risk custome
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated alerts for significant changes in customer circumstances", "
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 257:
RiskId: 2438
ComplianceId: 3099
RiskTitle: Failure to Monitor High-Risk Customer Transactions
Criticality: Medium
PossibleDamage: Undetected financial crimes and regulatory violations
Category: Compliance
RiskType: Current
BusinessImpact: Increased exposure to financial crimes and regulatory fines
RiskDescription: Failure to monitor high-risk customer transactions may result in undetected financial c
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated transaction monitoring alerts for suspicious activities", "2": "
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 258:
RiskId: 2439
ComplianceId: 3100
RiskTitle: Failure to Conduct Timely Audits
Criticality: High
PossibleDamage: Undetected compliance issues, increased regulatory scrutiny, and potential legal co
Category: Compliance
RiskType: Current
BusinessImpact: Increased risk exposure, regulatory fines, reputational damage.
RiskDescription: Failure to conduct audits as required may result in undetected compliance issues and

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear audit schedule and allocate resources accordingly", "2": "Implem
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 259:
RiskId: 2440
ComplianceId: 3101
RiskTitle: Inadequate EDD Process Evaluation
Criticality: Medium
PossibleDamage: Ineffective EDD procedures, increased risk exposure, potential non-compliance with
Category: Compliance
RiskType: Current
BusinessImpact: Increased risk exposure, potential non-compliance with AML regulations.
RiskDescription: Inadequate evaluation may lead to ineffective EDD procedures, increased risk exposu
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update audit checklists and risk assessment tools to reflect regulatory c
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 260:
RiskId: 2441

ComplianceId: 3102
RiskTitle: Increased Exposure to Financial Crimes
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Compliance
RiskType: Current
BusinessImpact: Risk exposure to financial crimes and regulatory penalties
RiskDescription: Failure to conduct comprehensive risk assessments for high-risk customers may lead
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement enhanced monitoring procedures for high-risk customers", "2": "Provid
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 261:
RiskId: 2442
ComplianceId: 3103
RiskTitle: Undetected Suspicious Activities in High-Risk Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of customer trust.
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial and reputational damage, legal consequences.
RiskDescription: Failure to monitor high-risk customer transactions may result in undetected suspicious
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhanced transaction monitoring controls", "2": "Regular audits of monitoring proc

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 262:

RiskId: 2443

ComplianceId: 3104

RiskTitle: Inadequate Documentation Risk

Criticality: High

PossibleDamage: Inadequate documentation may lead to inadequate risk assessment and potential ex

Category: Compliance

RiskType: Inherent

BusinessImpact: May result in regulatory fines, reputational damage, and legal implications

RiskDescription: Failure to document detailed information on PEPs may result in inadequate risk asses

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement a standardized documentation template for consistency", "2": "Conduc

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 263:

RiskId: 2444

ComplianceId: 3105

RiskTitle: Inaccurate Information Gathering Risk

Criticality: Medium

PossibleDamage: Inaccurate information gathering may lead to misinformed risk assessments and pot

Category: Compliance
RiskType: Inherent
BusinessImpact: May result in regulatory fines, reputational damage, and legal implications
RiskDescription: Failure to conduct structured interviews with PEPs may result in inaccurate informatio
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop standardized interview questions for consistency", "2": "Provide training
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 264:
RiskId: 2445
ComplianceId: 3106
RiskTitle: Inadequate Documentation Collection
Criticality: High
PossibleDamage: Inadequate documentation collection may result in regulatory non-compliance and re
Category: Compliance
RiskType: Residual
BusinessImpact: Delayed onboarding, potential fines, reputational damage
RiskDescription: Failure to collect documentation at onboarding may lead to inadequate verification of
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reminders for documentation collection deadlines", "2": "Pr
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 265:
RiskId: 2446
ComplianceId: 3107
RiskTitle: Delayed Verification
Criticality: Medium
PossibleDamage: Delayed verification may lead to potential money laundering risks going undetected
Category: Compliance
RiskType: Residual
BusinessImpact: Increased compliance risks, regulatory penalties
RiskDescription: Client relationship managers and compliance teams must verify all collected documer
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated verification processes for efficiency", "2": "Assign dedicated
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 266:
RiskId: 2447
ComplianceId: 3108
RiskTitle: Increased Exposure to Money Laundering Risks
Criticality: High
PossibleDamage: Financial penalties, loss of reputation, regulatory sanctions
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal and financial consequences
RiskDescription: Failure to conduct comprehensive risk assessments may lead to high-risk customers

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures", "2": "Regularly update risk assessment tools
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 267:
RiskId: 2448
ComplianceId: 3109
RiskTitle: Undetected Suspicious Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory scrutiny, reputational harm
RiskDescription: Failure to detect and report suspicious activities can lead to severe consequences for
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced training on transaction monitoring", "2": "Regular review of monitoring p
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 268:
RiskId: 2449

ComplianceId: 3110
RiskTitle: Inaccurate Client Net Worth Information
Criticality: High
PossibleDamage: Financial losses and reputational damage
Category: Financial
RiskType: Residual
BusinessImpact: Potential default on loans or investments
RiskDescription: Incorrect client net worth information can lead to incorrect financial decisions and pote
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of client net worth information", "2": "Training on proper net worth v
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 269:
RiskId: 2450
ComplianceId: 3111
RiskTitle: Inaccurate Source of Wealth Information
Criticality: High
PossibleDamage: Legal penalties and reputational damage
Category: Legal
RiskType: Residual
BusinessImpact: Legal non-compliance and damage to reputation
RiskDescription: Incorrect client source of wealth information can lead to legal issues and reputational
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 64.8
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular audits of source of wealth information", "2": "Training on proper source of
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 270:
RiskId: 2451
ComplianceId: 3112
RiskTitle: Undetected Compliance Breaches
Criticality: High
PossibleDamage: Financial penalties, loss of reputation, legal actions
Category: Operational
RiskType: Inherent
BusinessImpact: Significant financial and reputational damage
RiskDescription: Failure to detect compliance breaches in high-risk clients due to inadequate monitorin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced system alerts and thresholds", "2": "Regular system updates and enha
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 271:
RiskId: 2452
ComplianceId: 3113
RiskTitle: Inaccurate Risk Assessments
Criticality: Medium
PossibleDamage: Compliance violations, financial penalties

Category: Operational

RiskType: Inherent

BusinessImpact: Financial losses due to inaccurate risk assessments

RiskDescription: Failure to update client information leading to incorrect risk assessments and compli

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Automated information update reminders", "2": "Regular client contact for update

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 272:

RiskId: 2453

ComplianceId: 3114

RiskTitle: Failure to Verify Customer Identity

Criticality: High

PossibleDamage: Potential money laundering or terrorist financing activities

Category: Compliance

RiskType: Inherent

BusinessImpact: Risk management department

RiskDescription: Failure to verify customer identity may result in facilitating illegal activities through the

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement robust identity verification procedures", "2": "Utilize third-party verificat

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 273:
RiskId: 2454
ComplianceId: 3115
RiskTitle: Failure to Assess Customer Business Activities
Criticality: High
PossibleDamage: Unknowingly facilitating illicit transactions
Category: Compliance
RiskType: Inherent
BusinessImpact: Risk management department
RiskDescription: Failure to assess high-risk customers' business activities may lead to the financial ins
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Utilize business intelligence tools for analysis", "2": "Conduct site visits for verifica
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 274:
RiskId: 2455
ComplianceId: 3116
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Increased risk exposure, regulatory scrutiny
RiskDescription: Failure to detect suspicious activities can lead to financial losses and regulatory non-c

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced staff training on transaction monitoring", "2": "Regular review of system
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 275:
RiskId: 2456
ComplianceId: 3117
RiskTitle: Delayed Investigation of Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Increased risk exposure, regulatory scrutiny
RiskDescription: Delayed investigation of suspicious activities can lead to financial losses and regulato
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear escalation procedures for flagged activities", "2": "Regular training
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 276:
RiskId: 2457

ComplianceId: 3118
RiskTitle: Undetected Money Laundering and Terrorist Financing Risks
Criticality: High
PossibleDamage: Financial penalties, reputational damage, regulatory sanctions
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased exposure to financial crimes and regulatory non-compliance
RiskDescription: Failure to conduct annual risk assessments may lead to undetected money launderin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated risk assessment tools", "2": "Provide regular training on risk
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 277:
RiskId: 2458
ComplianceId: 3119
RiskTitle: Operational Disruptions from Unidentified Risks
Criticality: Medium
PossibleDamage: Operational inefficiencies, financial losses, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Disruptions to operations, financial losses, regulatory scrutiny
RiskDescription: Failure to conduct triggered risk assessments for significant changes may lead to ope
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish a clear process for identifying and triggering additional risk assessments

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 278:

RiskId: 2459

ComplianceId: 3120

RiskTitle: Misalignment of Risk Appetite Statement

Criticality: High

PossibleDamage: Increased exposure to risks not aligned with strategic objectives

Category: Operational

RiskType: Current

BusinessImpact: Potential financial losses, reputational damage, and operational disruptions

RiskDescription: Failure to update the risk appetite statement annually or after significant changes may

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly scheduled reviews by Executive Management Team and Risk Manager

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 279:

RiskId: 2460

ComplianceId: 3121

RiskTitle: Lack of Stakeholder Engagement

Criticality: Medium

PossibleDamage: Risk appetite statement not accurately reflecting organizational objectives and risk to

Category: Operational
RiskType: Current
BusinessImpact: Potential misalignment with strategic objectives and regulatory requirements
RiskDescription: Failure to engage stakeholders in developing the risk appetite statement may result in
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a structured stakeholder engagement process", "2": "Provide training to
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 280:
RiskId: 2461
ComplianceId: 3122
RiskTitle: Failure to Conduct EDD on High-Risk Clients
Criticality: High
PossibleDamage: Potential money laundering activities, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance, Legal, Reputational
RiskDescription: Failure to conduct EDD on high-risk clients may expose the organization to regulatory
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated EDD tools for efficient data collection", "2": "Provide regula
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 281:
RiskId: 2462
ComplianceId: 3123
RiskTitle: Failure to Review EDD for High-Risk Clients Annually
Criticality: Medium
PossibleDamage: Undetected suspicious activities, regulatory violations, financial losses
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance, Legal, Financial
RiskDescription: Failure to review EDD for high-risk clients annually may result in missed red flags or s
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated EDD review processes", "2": "Establish clear criteria for trig
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 282:
RiskId: 2463
ComplianceId: 3124
RiskTitle: Failure to Detect Suspicious Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal actions
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory scrutiny, loss of client trust
RiskDescription: Undetected suspicious transactions can lead to severe financial and reputational cons

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced training for monitoring analysts", "2": "Regular system upgrades for imp
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 283:
RiskId: 2464
ComplianceId: 3125
RiskTitle: Delayed Review of Flagged Transactions
Criticality: Medium
PossibleDamage: Regulatory fines, reputational damage, increased compliance risk
Category: Operational
RiskType: Current
BusinessImpact: Increased exposure to money laundering activities, regulatory scrutiny
RiskDescription: Delayed review of flagged transactions can lead to missed suspicious activities and p
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated alerts for timely reviews", "2": "Established escalation process for unre
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 284:
RiskId: 2465

ComplianceId: 3126
RiskTitle: Failure to Comply with AML Training Requirements
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, increased risk of money laundering activities
Category: Compliance
RiskType: Current
BusinessImpact: Private banking and wealth management operations
RiskDescription: Non-compliance with AML training requirements can lead to staff being unaware of re
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of staff training completion records", "2": "Implementing conse
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 285:
RiskId: 2466
ComplianceId: 3127
RiskTitle: Inadequate EDD Training
Criticality: High
PossibleDamage: Increased risk of regulatory violations, financial losses, and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, loss of client trust, damage to the organization's reputation
RiskDescription: Failure to provide adequate EDD training may lead to staff overlooking red flags, misi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular monitoring of training completion and understanding", "2": "Implementing

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 286:

RiskId: 2467

ComplianceId: 3128

RiskTitle: Delayed New Hire EDD Training

Criticality: Medium

PossibleDamage: Increased risk of non-compliance, errors in due diligence, and operational inefficienc

Category: Compliance

RiskType: Inherent

BusinessImpact: Potential delays in client onboarding, increased errors in due diligence processes, an

RiskDescription: Failure to provide timely EDD training to new hires may result in gaps in knowledge, l

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Automated onboarding process to ensure timely training", "2": "Assigning mentors

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 287:

RiskId: 2468

ComplianceId: 3129

RiskTitle: Undetected Suspicious Activities

Criticality: High

PossibleDamage: Regulatory fines, reputational damage

Category: Compliance
RiskType: Current
BusinessImpact: Private banking division
RiskDescription: Failure to detect suspicious activities in transactions of high-risk clients may lead to se
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on how to use the monitoring system effectively", "2": "Pe
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 288:
RiskId: 2469
ComplianceId: 3130
RiskTitle: Inaccurate Customer Profiles
Criticality: High
PossibleDamage: Inadequate risk assessment and potential exposure to financial crimes
Category: Operational
RiskType: Residual
BusinessImpact: Increased compliance violations, legal repercussions, and reputational damage
RiskDescription: Failure to update customer profiles may result in inaccurate risk assessments and exp
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated data collection processes", "2": "Provide regular training to
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 289:
RiskId: 2470
ComplianceId: 3131
RiskTitle: Unverified Customer Profiles
Criticality: Medium
PossibleDamage: Reliance on inaccurate data for risk assessment
Category: Operational
RiskType: Residual
BusinessImpact: Increased compliance violations and legal repercussions
RiskDescription: Failure to verify customer profile information may lead to reliance on inaccurate data f
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated verification processes", "2": "Regularly update verification p
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 290:
RiskId: 2471
ComplianceId: 3132
RiskTitle: Failure to Detect Money Laundering Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory scrutiny, reputational harm
RiskDescription: Failure to detect money laundering activities can result in severe financial and legal c

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced transaction monitoring tools", "2": "Regular training for monitoring team
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 291:
RiskId: 2472
ComplianceId: 3133
RiskTitle: Inadequate Monthly Transaction Review
Criticality: Medium
PossibleDamage: Missed suspicious activities, regulatory non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Potential regulatory fines, reputational damage, compliance issues
RiskDescription: Failure to conduct effective monthly transaction reviews may result in missed suspicio
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enhanced review processes", "2": "Regular training for review team", "3": "Automa
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 292:
RiskId: 2473

ComplianceId: 3134
RiskTitle: Outdated Risk Assessment
Criticality: High
PossibleDamage: Unidentified risks leading to potential financial losses or regulatory non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: All business units within the financial institution
RiskDescription: Failure to update the risk assessment document annually may result in key risks not b
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for compliance officers on risk assessment best practic
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 293:
RiskId: 2474
ComplianceId: 3135
RiskTitle: Inadequate Staff Training
Criticality: High
PossibleDamage: Errors in EDD processes, non-compliance with regulations, financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: Increased risk of financial losses, regulatory fines, reputational damage
RiskDescription: Lack of adequate training may result in staff errors, non-compliance with regulations,
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular monitoring of staff performance and feedback sessions", "2": "Additional

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 294:

RiskId: 2475

ComplianceId: 3136

RiskTitle: Outdated Staff Knowledge

Criticality: Medium

PossibleDamage: Increased errors, non-compliance with regulations

Category: Operational

RiskType: Inherent

BusinessImpact: Increased risk of errors, non-compliance

RiskDescription: Failure to conduct annual training may result in outdated knowledge, errors in EDD pr

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Automated reminders for training sessions", "2": "Regular assessments to identify

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 295:

RiskId: 2476

ComplianceId: 3137

RiskTitle: Non-Compliance with Record-Keeping Standards

Criticality: High

PossibleDamage: Regulatory fines, penalties, and reputational damage

Category: Compliance
RiskType: Residual
BusinessImpact: Potential financial losses and damage to reputation
RiskDescription: Failure to maintain accurate records may result in regulatory non-compliance and ass
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of records to ensure accuracy", "2": "Employee training on record-
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 296:
RiskId: 2477
ComplianceId: 3138
RiskTitle: Non-Compliance with Record Retention Requirements
Criticality: Medium
PossibleDamage: Non-compliance penalties and regulatory scrutiny
Category: Compliance
RiskType: Residual
BusinessImpact: Potential financial losses and regulatory sanctions
RiskDescription: Failure to retain records for the required duration may lead to regulatory non-compliar
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement record retention policies and procedures", "2": "Regularly review and u
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 297:
RiskId: 2478
ComplianceId: 3139
RiskTitle: Undetected Suspicious Activities
Criticality: High
PossibleDamage: Financial losses and regulatory penalties
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Failure to detect suspicious activities of high-risk customers can lead to financial losse
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular system updates and testing", "2": "Enhanced staff training on transaction
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 298:
RiskId: 2479
ComplianceId: 3140
RiskTitle: Lack of Daily Reviews
Criticality: Medium
PossibleDamage: Undetected suspicious activities and regulatory non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, regulatory penalties
RiskDescription: Failure to conduct daily reviews of flagged transactions can result in undetected suspi

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear review procedures", "2": "Assign dedicated staff for daily reviews",
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 299:
RiskId: 2480
ComplianceId: 3141
RiskTitle: Outdated High-Risk Customer Profiles
Criticality: High
PossibleDamage: Increased exposure to financial crimes
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines and reputational damage
RiskDescription: Outdated customer profiles may lead to missed suspicious activities and regulatory no
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for CDD team on EDD requirements", "2": "Automated alerts for p
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 300:
RiskId: 2481

ComplianceId: 3142
RiskTitle: Non-compliance with Annual Audit of EDD Processes
Criticality: High
PossibleDamage: Potential regulatory penalties and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units involved in EDD processes may be impacted by regulatory fines or
RiskDescription: Failure to conduct annual audits of EDD processes may result in unidentified compliar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a detailed audit plan with clear objectives and scope", "2": "Engage rele
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 301:
RiskId: 2482
ComplianceId: 3143
RiskTitle: Non-compliance with Quarterly Follow-Up on Audit Recommendations
Criticality: Medium
PossibleDamage: Operational inefficiencies and compliance breaches
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units involved in EDD processes may experience delays in addressing c
RiskDescription: Failure to follow up on audit recommendations may result in unresolved compliance is
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish a structured follow-up process for tracking recommendations", "2": "Ass
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 302:
RiskId: 2483
ComplianceId: 3144
RiskTitle: Money Laundering Risk
Criticality: High
PossibleDamage: Risk of facilitating illegal financial activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial loss, regulatory fines, reputational damage
RiskDescription: Failure to verify source of funds increases the risk of money laundering activities goin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures for source of funds verification", "2": "Provide
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 303:
RiskId: 2484
ComplianceId: 3145
RiskTitle: Undisclosed Wealth Risk
Criticality: High
PossibleDamage: Risk of undisclosed wealth sources leading to illegal financial activities

Category: Compliance
RiskType: Inherent
BusinessImpact: Financial loss, legal liabilities, reputational damage
RiskDescription: Failure to verify source of wealth increases the risk of clients engaging in illegal financ
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 77.35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures for source of wealth verification", "2": "Implem
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 304:
RiskId: 2485
ComplianceId: 3146
RiskTitle: Inadequate Customer Risk Assessment
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, and increased exposure to financial crimes.
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny and potential legal actions.
RiskDescription: Failure to properly assess customer risk profiles may result in onboarding high-risk cu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced training on risk assessment procedures", "2": "Regular reviews of risk a
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 305:
RiskId: 2486
ComplianceId: 3147
RiskTitle: Failure to Detect Suspicious Transactions
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, reputational damage
RiskDescription: The risk of not detecting suspicious transactions could lead to severe financial and re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust transaction monitoring systems", "2": "Provide regular training t
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 306:
RiskId: 2487
ComplianceId: 3148
RiskTitle: Failure to Identify Changes in Customer Risk Profiles
Criticality: Medium
PossibleDamage: Increased exposure to risk, regulatory non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: Increased exposure to risk, regulatory non-compliance
RiskDescription: Not identifying changes in customer risk profiles could lead to increased exposure to r

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement regular risk assessment procedures", "2": "Utilize automated risk scori
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 307:
RiskId: 2488
ComplianceId: 3149
RiskTitle: Inaccurate Client Net Worth Data
Criticality: High
PossibleDamage: Incorrect risk assessment, regulatory non-compliance, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Potential fines, reputational damage, legal actions
RiskDescription: Failure to collect accurate net worth information may lead to incorrect risk assessmen
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement training programs for staff on effective interview techniques", "2": "Impl
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 308:
RiskId: 2489

ComplianceId: 3150
RiskTitle: Unverified Wealth Source
Criticality: Medium
PossibleDamage: Exposure to money laundering risks, regulatory sanctions, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Legal actions, financial losses, reputational damage
RiskDescription: Failure to verify the source of wealth may lead to exposure to money laundering risks
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 38
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement robust internal controls for source verification", "2": "Conduct periodic a
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 309:
RiskId: 2490
ComplianceId: 3151
RiskTitle: Money Laundering Risk
Criticality: High
PossibleDamage: Increased regulatory scrutiny, fines, and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial losses, legal consequences, damage to reputation
RiskDescription: Failure to verify the source of wealth may result in high-risk clients using the financial
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence for high-risk clients", "2": "Regular audits of verification p
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 310:
RiskId: 2491
ComplianceId: 3152
RiskTitle: Failure to Verify Customer Identities
Criticality: High
PossibleDamage: Potential money laundering activities, identity theft, or fraud
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Failure to verify customer identities may lead to unauthorized account access, money
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated identity verification systems", "2": "Provide regular training
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 311:
RiskId: 2492
ComplianceId: 3153
RiskTitle: Lack of Ongoing Customer Due Diligence Monitoring
Criticality: Medium
PossibleDamage: Non-compliance with regulations, unidentified high-risk customers

Category: Operational
RiskType: Inherent
BusinessImpact: Regulatory fines, reputational damage
RiskDescription: Failure to conduct ongoing customer due diligence monitoring may result in non-comp
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated monitoring systems for customer risk assessment", "2": "Es
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 312:
RiskId: 2493
ComplianceId: 3154
RiskTitle: Failure to Implement EDD Measures for High-Risk Customers
Criticality: High
PossibleDamage: Increased exposure to financial crimes and regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal and regulatory sanctions, damage to reputation
RiskDescription: Failure to implement EDD measures for high-risk customers can result in increased e
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced staff training on EDD procedures", "2": "Regular audits and reviews of
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 313:
RiskId: 2494
ComplianceId: 3155
RiskTitle: Failure to Report Suspicious Activities
Criticality: High
PossibleDamage: Legal penalties, financial losses, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal and financial consequences for the organization
RiskDescription: Failure to report suspicious activities may result in money laundering or terrorist finan
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide regular training to employees on identifying and reporting suspicious activ
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 314:
RiskId: 2495
ComplianceId: 3156
RiskTitle: Failure to Verify Customer Identification Documents
Criticality: High
PossibleDamage: Identity theft, fraudulent transactions
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial losses
RiskDescription: Failure to verify customer identification documents may result in unauthorized access

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated verification tools", "2": "Conduct manual checks for suspici
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 315:
RiskId: 2496
ComplianceId: 3157
RiskTitle: Failure to Conduct EDD for High-Risk Customers
Criticality: Critical
PossibleDamage: Money laundering, terrorist financing
Category: Financial
RiskType: Current
BusinessImpact: Regulatory fines, reputational damage
RiskDescription: Failure to conduct EDD for high-risk customers may result in facilitating illegal financia
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement risk-based approach for EDD", "2": "Leverage automated transaction m
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 316:
RiskId: 2497

ComplianceId: 3158
RiskTitle: Failure to Detect Money Laundering Activities
Criticality: High
PossibleDamage: Increased risk of regulatory fines and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Compliance department and overall business operations
RiskDescription: Failure to detect money laundering activities can lead to severe regulatory consequen
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust transaction monitoring systems", "2": "Provide regular training t
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 317:
RiskId: 2498
ComplianceId: 3159
RiskTitle: Inaccurate Customer Information
Criticality: High
PossibleDamage: Inaccurate customer information leading to compliance breaches and increased risk
Category: Compliance
RiskType: Current
BusinessImpact: Compliance department and overall business operations
RiskDescription: Failure to update customer information can result in compliance breaches and increas
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement automated systems for data refresh", "2": "Conduct regular training for
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 318:
RiskId: 2499
ComplianceId: 3160
RiskTitle: Failure to Verify Beneficial Owners
Criticality: High
PossibleDamage: Potential involvement in illicit activities due to unidentified beneficial owners.
Category: Compliance
RiskType: Current
BusinessImpact: Legal penalties, reputational damage, and financial losses.
RiskDescription: Failure to verify beneficial owners may result in non-compliance with regulations and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated beneficial owner verification processes", "2": "Enhance staf
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 319:
RiskId: 2500
ComplianceId: 3161
RiskTitle: Failure to Assess Legal Arrangements Legitimacy
Criticality: High
PossibleDamage: Unknowingly facilitating illegal activities due to inadequate assessment of legal arran

Category: Compliance
RiskType: Current
BusinessImpact: Legal penalties, reputational damage, and financial losses.
RiskDescription: Failure to assess the legitimacy of legal arrangements may result in non-compliance v
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures for assessing legal arrangements", "2": "Regu
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 320:
RiskId: 2501
ComplianceId: 3162
RiskTitle: Failure to Conduct Comprehensive EDD on PEPs
Criticality: High
PossibleDamage: Increased risk of money laundering or terrorist financing
Category: Compliance
RiskType: Current
BusinessImpact: Legal and financial penalties, reputational damage
RiskDescription: Failure to collect comprehensive information on PEPs may result in regulatory non-co
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures for PEPs", "2": "Implement automated monitor
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 321:
RiskId: 2502
ComplianceId: 3163
RiskTitle: Failure to Review PEP Profiles Annually
Criticality: Medium
PossibleDamage: Failure to detect changes in PEP risk levels
Category: Compliance
RiskType: Current
BusinessImpact: Increased exposure to financial crimes, regulatory scrutiny
RiskDescription: Neglecting annual reviews of PEP profiles may result in missed changes in risk levels
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enhance monitoring of PEP profiles", "2": "Establish clear escalation procedures f
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 322:
RiskId: 2503
ComplianceId: 3164
RiskTitle: Failure to Detect Suspicious PEP Transactions
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Increased risk exposure to financial crime and regulatory scrutiny
RiskDescription: Inadequate transaction monitoring may result in undetected suspicious activities invol

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance transaction monitoring systems", "2": "Regularly update PEP and sancti
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 323:
RiskId: 2504
ComplianceId: 3165
RiskTitle: Anomalies in Quarterly PEP Transaction Reviews
Criticality: Medium
PossibleDamage: Regulatory non-compliance, increased financial crime risk
Category: Operational
RiskType: Residual
BusinessImpact: Potential regulatory fines, reputational damage
RiskDescription: Inadequate quarterly reviews may result in undetected anomalies in PEP transactions
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enhance review procedures for PEP transactions", "2": "Regular training for comp
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 324:
RiskId: 2505

ComplianceId: 3166
RiskTitle: Failure to Identify High-Risk Customers
Criticality: High
PossibleDamage: Potential money laundering activities and regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial losses, reputational damage
RiskDescription: Failure to identify high-risk customers may result in facilitating illegal activities and reg
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance customer due diligence procedures", "2": "Implement transaction monito
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 325:
RiskId: 2506
ComplianceId: 3167
RiskTitle: Inaccurate Risk Assessment
Criticality: High
PossibleDamage: Inadequate risk mitigation strategies, regulatory non-compliance, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, regulatory sanctions, reputational damage
RiskDescription: Failure to accurately assess risks may lead to inadequate risk mitigation strategies an
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Conduct regular training for compliance staff on risk assessment review", "2": "Im
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 326:
RiskId: 2507
ComplianceId: 3168
RiskTitle: Outdated EDD Policies and Procedures
Criticality: High
PossibleDamage: Increased exposure to financial crimes and regulatory violations
Category: Compliance
RiskType: Current
BusinessImpact: Potential regulatory fines and reputational damage
RiskDescription: Failure to review EDD policies and procedures may result in outdated risk controls, le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust training program for staff on EDD policies and procedures", "2
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 327:
RiskId: 2508
ComplianceId: 3169
RiskTitle: Inadequate Staff Training
Criticality: High
PossibleDamage: Ineffective EDD processes, regulatory violations, fines or penalties

Category: Operational
RiskType: Inherent
BusinessImpact: All business units may be impacted by errors in EDD processes and potential regulat
RiskDescription: Failure to provide adequate staff training may result in staff lacking essential knowled
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of staff training completion status", "2": "Provide additional tra
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 328:
RiskId: 2509
ComplianceId: 3170
RiskTitle: Non-compliance with EDD Documentation Retention
Criticality: High
PossibleDamage: Regulatory fines, legal actions, and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential financial losses and damage to reputation
RiskDescription: Failure to retain EDD documentation as required by regulations may result in penaltie
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation retention policies", "2": "Automated reminders
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 329:
RiskId: 2510
ComplianceId: 3171
RiskTitle: Ineffective Implementation of Corrective Actions
Criticality: High
PossibleDamage: Potential recurrence of audit findings and regulatory non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: May lead to financial losses and reputational damage
RiskDescription: Failure to implement corrective actions effectively may result in the persistence of ide
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear accountability for corrective actions", "2": "Regular monitoring and
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 330:
RiskId: 2511
ComplianceId: 3172
RiskTitle: Incomplete Audit Coverage
Criticality: High
PossibleDamage: Regulatory penalties, reputational damage, increased compliance risks
Category: Operational
RiskType: Current
BusinessImpact: Disruption of audit processes, financial losses, regulatory sanctions
RiskDescription: Failure to conduct annual audit planning may result in incomplete audit coverage, lea

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular communication and coordination between audit team, compliance, and ri
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 331:
RiskId: 2512
ComplianceId: 3173
RiskTitle: Inadequate Auditor Qualifications
Criticality: High
PossibleDamage: Inaccurate EDD audits, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Human Resources and Compliance departments
RiskDescription: The risk of auditors lacking proper qualifications may result in incomplete or inaccurat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update qualification standards based on industry best practi
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 332:
RiskId: 2513

ComplianceId: 3174
RiskTitle: Delayed Audit Reporting
Criticality: High
PossibleDamage: Operational disruptions, compliance failures, and reputational damage.
Category: Operational
RiskType: Residual
BusinessImpact: Potential delays in addressing compliance issues and implementing corrective actions
RiskDescription: Failure to submit audit reports on time may lead to prolonged exposure to identified ri
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting deadlines and consequences for non-compliance.", "2": "
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 333:
RiskId: 2514
ComplianceId: 3175
RiskTitle: Failure to Conduct Enhanced Due Diligence on High-Risk Clients
Criticality: High
PossibleDamage: Increased risk of money laundering activities going undetected, leading to regulatory
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal and financial consequences, damage to reputation
RiskDescription: Failure to conduct enhanced due diligence on high-risk clients may result in the bank
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement robust EDD procedures and training programs", "2": "Regularly review

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 334:

RiskId: 2515

ComplianceId: 3176

RiskTitle: Missed Money Laundering Activities

Criticality: High

PossibleDamage: Regulatory fines, reputational damage

Category: Operational

RiskType: Inherent

BusinessImpact: Potential regulatory investigations, financial penalties, and damage to the bank's repu

RiskDescription: Failure to identify and report money laundering activities due to inadequate training co

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhanced training programs", "2": "Regular audits of reported activities", "3": "Enc

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 335:

RiskId: 2516

ComplianceId: 3177

RiskTitle: Lack of Awareness on AML Regulations

Criticality: Medium

PossibleDamage: Missed suspicious activities, regulatory non-compliance

Category: Operational

RiskType: Inherent

BusinessImpact: Increased risk of regulatory fines, reputational damage, and potential legal actions du

RiskDescription: Failure to provide regular updates on AML regulations and red flags may result in staf

RiskLikelihood: 5

RiskImpact: 7

RiskExposureRating: 35

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Continuous training and updates", "2": "Regular assessments of staff knowledge",

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 336:

RiskId: 2517

ComplianceId: 3178

RiskTitle: Identity Theft and Money Laundering Risk

Criticality: High

PossibleDamage: Financial losses, reputational damage, legal consequences

Category: Compliance

RiskType: Inherent

BusinessImpact: Potential financial losses and damage to reputation.

RiskDescription: Failure to verify customer documentation may lead to unauthorized account access, id

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement automated verification tools", "2": "Conduct manual checks against trus

CreatedAt: 2025-11-14 00:00:00

CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 337:
RiskId: 2518
ComplianceId: 3179
RiskTitle: Money Laundering and Terrorist Financing Risk
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential financial losses and damage to reputation.
RiskDescription: Failure to assess high-risk customers may lead to illicit financial activities, regulatory v
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct enhanced due diligence on high-risk customers", "2": "Review transactio
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 338:
RiskId: 2519
ComplianceId: 3180
RiskTitle: Failure to Detect Suspicious Transactions
Criticality: High
PossibleDamage: Financial penalties, regulatory sanctions, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of business operations, financial losses
RiskDescription: Inability to detect suspicious transactions may lead to severe consequences for the in

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced staff training on transaction monitoring", "2": "Regular system audits ar
CreatedAt: 2025-11-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 339:
RiskId: 2208
ComplianceId: 2870
RiskTitle: Delayed Detection of Suspicious PEP Transactions
Criticality: Medium
PossibleDamage: Delayed detection of illicit activities or money laundering
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Delayed detection of suspicious PEP transactions could lead to financial losses and r
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement real-time transaction monitoring alerts", "2": "Establish clear review tim
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 340:
RiskId: 2209

ComplianceId: 2871
RiskTitle: Failure to Collect and Verify Customer Information
Criticality: High
PossibleDamage: Increased risk of money laundering, fraud, and regulatory non-compliance
Category: Compliance
RiskType: Residual
BusinessImpact: Potential regulatory fines, loss of reputation, legal actions
RiskDescription: Failure to collect and verify necessary customer information may lead to increased ris
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust automated systems for data collection and verification", "2": "Tr
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 341:
RiskId: 2210
ComplianceId: 2872
RiskTitle: Undetected Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Disruption to business operations, financial losses
RiskDescription: Failure to detect suspicious activities through quarterly transaction reviews may result
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhance transaction monitoring systems", "2": "Provide regular training to staff or

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 342:

RiskId: 2211

ComplianceId: 2873

RiskTitle: Real-Time Monitoring Failure

Criticality: High

PossibleDamage: Financial losses, regulatory fines, reputational damage

Category: Compliance

RiskType: Residual

BusinessImpact: Disruption to business operations, financial losses

RiskDescription: Inadequate real-time monitoring of customer transactions may result in delayed detec

RiskLikelihood: 9

RiskImpact: 9

RiskExposureRating: 81

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement real-time transaction monitoring systems", "2": "Enhance anomaly dete

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 343:

RiskId: 2212

ComplianceId: 2874

RiskTitle: Failure to Verify Customer Identification Information

Criticality: High

PossibleDamage: Identity theft, fraud, regulatory fines

Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial losses
RiskDescription: Failure to verify customer identification information may lead to unauthorized account
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust verification procedures", "2": "Regularly update verification tools
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 344:
RiskId: 2213
ComplianceId: 2875
RiskTitle: Lack of Documentation in Verification Process
Criticality: Medium
PossibleDamage: Regulatory non-compliance, legal issues
Category: Operational
RiskType: Current
BusinessImpact: Audit failures, legal disputes
RiskDescription: Failure to document the customer verification process may lead to regulatory fines, le
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement robust documentation procedures", "2": "Regularly review and update
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 345:
RiskId: 2214
ComplianceId: 2876
RiskTitle: Undetected Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Risk Management, Compliance Department
RiskDescription: Failure to detect suspicious activities in real-time may result in severe financial and re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular staff training on monitoring procedures", "2": "Automated alerts for flagge
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 346:
RiskId: 2215
ComplianceId: 2877
RiskTitle: Delayed Review of Flagged Transactions
Criticality: Medium
PossibleDamage: Missed opportunities to identify suspicious activities, compliance breaches
Category: Compliance
RiskType: Inherent
BusinessImpact: Risk Management, Compliance Department
RiskDescription: Failure to review flagged transactions promptly may lead to missed opportunities to id

RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated alerts for daily reviews", "2": "Regular staff training on review procedu
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 347:
RiskId: 2216
ComplianceId: 2878
RiskTitle: Outdated Customer Information
Criticality: High
PossibleDamage: Incorrect decisions, financial losses, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Customer service disruptions, compliance violations, financial risks
RiskDescription: Failure to refresh customer information annually may result in outdated records, leadi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reminders for annual information refresh", "2": "Provide trai
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 348:
RiskId: 2217

ComplianceId: 2879
RiskTitle: Delayed Information Refresh Completion
Criticality: Medium
PossibleDamage: Outdated records, compliance issues
Category: Operational
RiskType: Inherent
BusinessImpact: Customer service disruptions, regulatory fines
RiskDescription: Delays in completing information refreshes may result in outdated records, leading to
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish escalation procedures for overdue refreshes", "2": "Monitor and report o
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 349:
RiskId: 2218
ComplianceId: 2880
RiskTitle: Failure to Identify PEPs
Criticality: High
PossibleDamage: Financial penalties, reputational damage, and regulatory sanctions
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny and potential loss of business opportunities
RiskDescription: Failure to identify PEPs can lead to unknowingly engaging in high-risk business relati
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training for compliance officers on PEP identification procedures", "2": "In

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 350:

RiskId: 2219

ComplianceId: 2881

RiskTitle: Failure to Review PEP Status

Criticality: Medium

PossibleDamage: Regulatory fines, increased exposure to financial crime

Category: Compliance

RiskType: Inherent

BusinessImpact: Increased regulatory scrutiny and potential financial losses

RiskDescription: Failure to review PEP status regularly can lead to missed changes in risk levels and i

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement automated alerts for significant changes in customer circumstances", "

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 351:

RiskId: 2220

ComplianceId: 2882

RiskTitle: Undetected Suspicious Activities in PEP Transactions

Criticality: High

PossibleDamage: Potential regulatory fines, financial losses, and reputational damage

Category: Operational
RiskType: Current
BusinessImpact: All business units involved in transaction processing
RiskDescription: Failure to detect suspicious activities in PEP transactions may result in regulatory viol
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced transaction monitoring procedures", "2": "Regular audits of PEP transa
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 352:
RiskId: 2221
ComplianceId: 2883
RiskTitle: Delayed Detection of Suspicious Activities in PEP Transactions
Criticality: Medium
PossibleDamage: Regulatory scrutiny and financial losses
Category: Operational
RiskType: Current
BusinessImpact: All business units involved in transaction processing
RiskDescription: Failure to timely review flagged PEP transactions may result in regulatory scrutiny an
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear escalation procedures for flagged activities", "2": "Regular training
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 353:
RiskId: 2222
ComplianceId: 2884
RiskTitle: Inadequate Client Suitability Assessment
Criticality: High
PossibleDamage: Financial losses, regulatory penalties, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Compliance breaches, financial losses, reputational damage
RiskDescription: Failure to conduct thorough client suitability assessments may result in providing unsu
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement training programs for compliance officers and relationship managers o
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 354:
RiskId: 2223
ComplianceId: 2885
RiskTitle: Failure to Identify Financial Crime Risks
Criticality: High
PossibleDamage: Increased risk of financial crime incidents and regulatory non-compliance
Category: Compliance
RiskType: Inherent
BusinessImpact: Private Banking
RiskDescription: Staff may not be equipped to identify red flags and potential financial crime risks, lead

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of staff training completion", "2": "Provide additional support a
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 355:
RiskId: 2224
ComplianceId: 2886
RiskTitle: Outdated Knowledge on Financial Crime Risks
Criticality: Medium
PossibleDamage: Outdated knowledge leading to missed red flags and increased risk exposure
Category: Compliance
RiskType: Inherent
BusinessImpact: Private Banking
RiskDescription: Staff may fail to recognize new trends and risks in financial crime, leading to increase
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated reminders for staff to complete refresher training", "2": "Provide incent
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 356:
RiskId: 2225

ComplianceId: 2887
RiskTitle: High-Value Transaction Risk
Criticality: High
PossibleDamage: Financial loss, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of client trust, regulatory scrutiny
RiskDescription: Risk of approving high-value transactions without proper assessment leading to finan
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence for high-risk transactions", "2": "Regular training for staff
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 357:
RiskId: 2226
ComplianceId: 2888
RiskTitle: Cross-Border Transaction Risk
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of license
Category: Operational
RiskType: Current
BusinessImpact: Increased compliance costs, loss of international business
RiskDescription: Risk of facilitating cross-border transactions without proper risk assessment leading t
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhanced due diligence for cross-border transactions", "2": "Regular audits of cro

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 358:

RiskId: 2227

ComplianceId: 2889

RiskTitle: Misvaluation of High-Value Assets

Criticality: High

PossibleDamage: Financial losses, reputational damage, regulatory fines

Category: Operational

RiskType: Current

BusinessImpact: Internal Audit Department, Compliance Officer

RiskDescription: Incorrect valuation of high-value assets leading to financial losses and reputational da

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement regular audits", "2": "Review audit findings with senior management", "

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 359:

RiskId: 2228

ComplianceId: 2890

RiskTitle: Misuse of High-Value Assets in Significant Transactions

Criticality: Medium

PossibleDamage: Financial losses, reputational damage, regulatory fines

Category: Operational
RiskType: Current
BusinessImpact: Internal Audit Department, Compliance Officer
RiskDescription: Potential misuse of high-value assets in significant transactions leading to financial los
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Review significant transactions promptly", "2": "Implement additional reviews as n
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 360:
RiskId: 2229
ComplianceId: 2891
RiskTitle: Failure to Verify Customer Documentation
Criticality: High
PossibleDamage: Money laundering, fraud, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial losses, legal consequences, damage to reputation
RiskDescription: Failure to verify customer documentation may result in facilitating illegal activities, fina
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust verification procedures", "2": "Provide regular training to staff or
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 361:
RiskId: 2230
ComplianceId: 2892
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Increased risk exposure to financial crimes
RiskDescription: Failure to detect suspicious activities can result in regulatory violations and damage to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance automated monitoring systems", "2": "Provide ongoing training to staff",
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 362:
RiskId: 2231
ComplianceId: 2893
RiskTitle: Delayed Detection of Suspicious Activities in High-Risk Accounts
Criticality: Medium
PossibleDamage: Regulatory non-compliance, increased financial crime risk
Category: Operational
RiskType: Current
BusinessImpact: Increased exposure to financial crimes and regulatory penalties
RiskDescription: Delayed detection of suspicious activities in high-risk accounts can lead to regulatory

RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enhance review procedures for high-risk accounts", "2": "Implement automated al
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 363:
RiskId: 2232
ComplianceId: 2894
RiskTitle: Misuse of Complex Legal Structures
Criticality: High
PossibleDamage: Financial crimes, regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial losses, regulatory scrutiny, reputational damage
RiskDescription: Failure to properly identify and verify beneficial owners may lead to the misuse of com
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust customer due diligence procedures", "2": "Regularly update ben
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 364:
RiskId: 2233

ComplianceId: 2895
RiskTitle: Non-Compliance with Legal Arrangements Assessment
Criticality: High
PossibleDamage: Legal and reputational damage, regulatory fines
Category: Legal
RiskType: Residual
BusinessImpact: Legal and compliance departments may face penalties and loss of credibility
RiskDescription: Failure to assess legal arrangements could lead to non-compliance with regulations a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence procedures", "2": "Regular legal reviews", "3": "Training f
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 365:
RiskId: 2234
ComplianceId: 2896
RiskTitle: Failure to Detect Unusual Activity in Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Increased regulatory scrutiny, loss of customer trust, financial penalties
RiskDescription: The risk of not detecting unusual activity in transactions associated with complex lega
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly update and calibrate the automated monitoring systems", "2": "Provide
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 366:
RiskId: 2235
ComplianceId: 2897
RiskTitle: Missed Detection of Financial Crime in Manual Reviews
Criticality: Medium
PossibleDamage: Regulatory fines, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Increased regulatory scrutiny, loss of customer trust, financial penalties
RiskDescription: The risk of not conducting thorough manual reviews of flagged transactions, leading t
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear review procedures and guidelines for the compliance team", "2": "I
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 367:
RiskId: 2236
ComplianceId: 2898
RiskTitle: Incomplete Risk Assessment Documentation
Criticality: High
PossibleDamage: Non-compliance with regulatory requirements, increased exposure to risks

Category: Compliance
RiskType: Current
BusinessImpact: Potential regulatory fines, reputational damage, and operational disruptions
RiskDescription: Failure to review the risk assessment documentation may result in missing critical risk
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular training for auditors on risk assessment review processes", "2": "
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 368:
RiskId: 2237
ComplianceId: 2899
RiskTitle: Non-alignment of Policies with Risk Assessment
Criticality: High
PossibleDamage: Ineffective risk mitigation, potential regulatory violations, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Audit department, Compliance department
RiskDescription: Failure to align policies with the risk assessment may result in ineffective risk mitigatio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of policies based on risk assessment findings", "2": "T
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 369:
RiskId: 2238
ComplianceId: 2900
RiskTitle: Inaccurate Customer-Specific Profiles
Criticality: Medium
PossibleDamage: Inadequate risk assessment, exposure to high-risk customers, potential regulatory s
Category: Operational
RiskType: Inherent
BusinessImpact: Audit department, Customer Service department
RiskDescription: Inability to develop accurate customer-specific profiles based on EDD policies and pro
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Training for staff on customer profiling techniques", "2": "Regular review of custom
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 370:
RiskId: 2239
ComplianceId: 2901
RiskTitle: Inadequate Staff Training
Criticality: High
PossibleDamage: Errors in EDD processes, compliance violations, financial penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Impact on EDD processes and regulatory compliance
RiskDescription: Insufficient training may result in staff lacking the necessary knowledge and skills to e

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training assessments and updates", "2": "Providing additional training res
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 371:
RiskId: 2240
ComplianceId: 2902
RiskTitle: Inaccurate Evaluation of Knowledge Testing Results
Criticality: Medium
PossibleDamage: Overlooking gaps in staff training, compliance issues
Category: Operational
RiskType: Inherent
BusinessImpact: Impact on EDD processes and regulatory compliance
RiskDescription: Failure to accurately evaluate knowledge testing results may result in staff not posses
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing standardized testing procedures", "2": "Providing remedial training f
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 372:
RiskId: 2241

ComplianceId: 2903
RiskTitle: Inaccurate EDD Documentation
Criticality: High
PossibleDamage: Incorrect risk assessments, regulatory fines, and reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Impact on audit department operations and organizational compliance
RiskDescription: Failure to maintain accurate EDD documentation may result in incorrect risk assessm
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for auditors on record-keeping requirements", "2": "Implement au
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 373:
RiskId: 2242
ComplianceId: 2904
RiskTitle: Failure to Implement Audit Recommendations
Criticality: High
PossibleDamage: Recurring issues, financial losses, and reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units may be impacted
RiskDescription: Failure to track and implement audit recommendations may result in unresolved issue
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear accountability for tracking and implementing recommendations", "2

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 374:

RiskId: 2243

ComplianceId: 2905

RiskTitle: Failure to Implement Enhanced Due Diligence Measures

Criticality: High

PossibleDamage: Financial losses, reputational damage, regulatory fines

Category: Compliance

RiskType: Inherent

BusinessImpact: Potential legal and financial consequences for the organization

RiskDescription: Failure to implement enhanced due diligence measures may result in high-risk transa

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training for staff on EDD procedures", "2": "Automated alerts for high-risk

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 375:

RiskId: 2244

ComplianceId: 2906

RiskTitle: Undetected High-Risk Transactions

Criticality: High

PossibleDamage: Financial losses, regulatory fines, reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, regulatory penalties, reputational damage
RiskDescription: Failure to detect and report high-risk transactions can result in financial losses, regula
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated alerts for high-risk transactions", "2": "Conduct regular train
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 376:
RiskId: 2245
ComplianceId: 2907
RiskTitle: Inadequate Reporting of Suspicious Activities
Criticality: High
PossibleDamage: Legal and regulatory consequences
Category: Operational
RiskType: Inherent
BusinessImpact: Legal and regulatory penalties, reputational damage
RiskDescription: Failure to report suspicious activities in a timely manner can result in legal and regula
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting procedures and escalation paths", "2": "Conduct regular
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 377:
RiskId: 2246
ComplianceId: 2908
RiskTitle: Failure to Conduct Customer Risk Assessments
Criticality: High
PossibleDamage: Exposure to high ML/TF risks and regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased risk exposure and potential legal consequences
RiskDescription: Failure to conduct customer risk assessments may lead to unknowingly engaging with
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated risk assessment tools", "2": "Regular training for staff on ris
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 378:
RiskId: 2247
ComplianceId: 2909
RiskTitle: Inadequate Due Diligence Checklist
Criticality: High
PossibleDamage: Potential exposure to ML/TF risks due to incomplete or ineffective due diligence mea
Category: Compliance
RiskType: Inherent
BusinessImpact: Legal and reputational consequences for the organization
RiskDescription: Failure to establish a comprehensive checklist for enhanced due diligence could resul

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of the checklist to incorporate any regulatory changes
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 379:
RiskId: 2248
ComplianceId: 2910
RiskTitle: Ineffective Transaction Monitoring
Criticality: High
PossibleDamage: Potential exposure to regulatory violations and reputational damage due to undetect
Category: Operational
RiskType: Inherent
BusinessImpact: Regulatory fines and reputational damage for the organization
RiskDescription: Failure to effectively utilize transaction monitoring systems could result in high-risk cu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on how to interpret and respond to alerts generated by th
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 380:
RiskId: 2249

ComplianceId: 2911
RiskTitle: Failure to Screen New Customers for Financial Sanctions
Criticality: High
PossibleDamage: Legal penalties, financial losses, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal and financial consequences
RiskDescription: Failure to screen new customers against financial sanctions lists could result in inadve
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated screening systems", "2": "Provide regular training on sancti
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 381:
RiskId: 2250
ComplianceId: 2912
RiskTitle: Failure to Screen Existing Customers Annually for Financial Sanctions
Criticality: High
PossibleDamage: Legal penalties, financial losses, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal and financial consequences
RiskDescription: Failure to screen existing customers annually against financial sanctions lists could re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 75.96
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement automated screening systems", "2": "Provide regular training on sancti
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 382:
RiskId: 2251
ComplianceId: 2913
RiskTitle: Failure to Conduct Comprehensive Risk Assessment
Criticality: High
PossibleDamage: Non-compliance with regulatory requirements, increased risk exposure
Category: Operational
RiskType: Inherent
BusinessImpact: Impact on reputation, financial stability, and regulatory standing
RiskDescription: Failure to conduct a comprehensive risk assessment may lead to improper applicatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Utilize risk assessment tools and methodologies", "2": "Ensure timely review of as
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 383:
RiskId: 2252
ComplianceId: 2914
RiskTitle: Non-compliance with Customer Due Diligence Timing Requirements
Criticality: High
PossibleDamage: Increased risk of regulatory fines and reputational damage

Category: Compliance
RiskType: Residual
BusinessImpact: Financial penalties and loss of customer trust
RiskDescription: Failure to adjust the timing of customer due diligence may result in regulatory violation
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on updated timing requirements", "2": "Automated alerts for overd
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 384:
RiskId: 2253
ComplianceId: 2915
RiskTitle: Inaccurate Customer Information Verification
Criticality: Medium
PossibleDamage: Increased risk of fraudulent activities and financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses and reputational damage
RiskDescription: Failure to verify the quality of customer information may result in fraudulent transactio
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on data verification processes", "2": "Implement automated data
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 385:
RiskId: 2254
ComplianceId: 2916
RiskTitle: Delayed Documentation Retrieval
Criticality: High
PossibleDamage: Regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and damage to reputation
RiskDescription: Failure to obtain necessary documentation from third parties in a timely manner may r
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication channels with third parties regarding documentatio
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 386:
RiskId: 2255
ComplianceId: 2917
RiskTitle: Non-Compliance with Third-Party Regulatory Requirements
Criticality: High
PossibleDamage: Legal penalties, reputational damage, regulatory sanctions
Category: Compliance
RiskType: Residual
BusinessImpact: Non-compliance may result in fines, legal actions, and damage to the organization's r
RiskDescription: Failure to obtain and maintain required documentation from third parties may lead to r

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update checklist of required documentation", "2": "Implemer
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 387:
RiskId: 2256
ComplianceId: 2918
RiskTitle: Inconsistent Application of Group-Level CDD and Record-Keeping Requirements
Criticality: High
PossibleDamage: Regulatory sanctions, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: All DNFBP operations involving group-affiliated third parties
RiskDescription: Failure to verify group-level CDD and record-keeping requirements may lead to non-c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of group compliance practices", "2": "Maintain records of complian
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 388:
RiskId: 2257

ComplianceId: 2919
RiskTitle: Failure to Detect Suspicious Activity
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal consequences
Category: Operational
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial losses, reputational damage
RiskDescription: Failure to detect suspicious activity may lead to money laundering or terrorist financin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on monitoring systems", "2": "Regular audits of monitorin
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 389:
RiskId: 2258
ComplianceId: 2920
RiskTitle: Delayed Alert Review
Criticality: Medium
PossibleDamage: Financial losses, regulatory penalties, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial losses, reputational damage
RiskDescription: Delayed review of alerts may result in missed suspicious activities, leading to financia
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish clear escalation procedures for flagged alerts", "2": "Regular training for
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 390:
RiskId: 2259
ComplianceId: 2921
RiskTitle: Failure to Conduct Enhanced Due Diligence
Criticality: High
PossibleDamage: Increased exposure to financial crimes and regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance function and overall organizational reputation
RiskDescription: Failure to conduct enhanced due diligence on high-risk customers may lead to regula
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence training for staff", "2": "Regular audits of due diligence pr
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 391:
RiskId: 2260
ComplianceId: 2922
RiskTitle: Failure to Conduct Periodic Enhanced Due Diligence Reviews
Criticality: Medium
PossibleDamage: Undetected changes in risk levels and exposure to financial crimes

Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance function and overall organizational reputation
RiskDescription: Failure to conduct periodic enhanced due diligence reviews may result in undetected
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated risk monitoring systems", "2": "Enhanced data analytics for risk detect
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 392:
RiskId: 2261
ComplianceId: 2923
RiskTitle: Undisclosed Source of Wealth
Criticality: High
PossibleDamage: Increased exposure to financial crimes and regulatory penalties.
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units involved in customer onboarding and compliance.
RiskDescription: Customers providing false or misleading information about their source of wealth coul
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced customer due diligence procedures.", "2": "Regular training for complia
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 393:
RiskId: 2262
ComplianceId: 2924
RiskTitle: Undetected Changes in Risk Profile
Criticality: Medium
PossibleDamage: Failure to detect changes in risk profile of high-risk customers.
Category: Compliance
RiskType: Residual
BusinessImpact: All business units involved in customer onboarding and compliance.
RiskDescription: Failure to conduct annual reviews of high-risk customers could result in undetected ch
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated review processes for high-risk customers.", "2": "Regular training for c
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 394:
RiskId: 2263
ComplianceId: 2925
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, and potential legal actions
Category: Operational
RiskType: Inherent
BusinessImpact: Compliance department
RiskDescription: Failure to detect suspicious activities through automated monitoring systems may res

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on how to use the monitoring systems effectively", "2": "F
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 395:
RiskId: 2264
ComplianceId: 2926
RiskTitle: Delayed Review of Flagged Transactions
Criticality: High
PossibleDamage: Regulatory scrutiny, potential penalties, and reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Compliance department
RiskDescription: Delayed review of flagged transactions may lead to non-compliance with reporting req
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear review procedures and escalation protocols for flagged transaction
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 396:
RiskId: 2265

ComplianceId: 2927
RiskTitle: Failure to Conduct Customer Risk Assessment
Criticality: High
PossibleDamage: Exposure to high-risk customers leading to financial losses or reputational damage.
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage.
RiskDescription: Failure to conduct risk assessments may result in exposure to high-risk customers, in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on risk assessment procedures", "2": "Implement automa
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 397:
RiskId: 2266
ComplianceId: 2928
RiskTitle: Undetected Suspicious Activities in High-Risk Accounts
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Increased exposure to financial crimes and potential damage to the organization's rep
RiskDescription: Failure to detect and investigate suspicious activities in high-risk accounts can lead to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhance transaction monitoring algorithms to improve detection accuracy", "2": "F

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 398:

RiskId: 2267

ComplianceId: 2929

RiskTitle: Inefficient Detection of Suspicious Activities

Criticality: Medium

PossibleDamage: Increased exposure to financial crimes, regulatory fines

Category: Operational

RiskType: Current

BusinessImpact: Missed detection of suspicious activities can result in financial losses and regulatory p

RiskDescription: Reliance on manual monitoring processes can lead to inefficiencies in detecting suspi

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly update and test the transaction monitoring algorithms for accuracy", "2"

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 399:

RiskId: 2268

ComplianceId: 2930

RiskTitle: Failure to Timely File SARs

Criticality: High

PossibleDamage: Legal penalties, reputational damage, increased risk of financial crime

Category: Compliance
RiskType: Current
BusinessImpact: Legal consequences, reputational harm
RiskDescription: Failure to file SARs promptly may lead to regulatory scrutiny, fines, and damage to th
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting procedures and escalation paths", "2": "Provide ongoing
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 400:
RiskId: 2269
ComplianceId: 2931
RiskTitle: Incomplete or Inaccurate SARs
Criticality: Medium
PossibleDamage: Hindered investigations, regulatory inquiries, increased risk of financial crime
Category: Compliance
RiskType: Current
BusinessImpact: Legal consequences, reputational harm
RiskDescription: Submitting incomplete or inaccurate SARs may impede investigations, attract regulato
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide training on completing the reporting template accurately", "2": "Implement
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 401:
RiskId: 2270
ComplianceId: 2932
RiskTitle: Inaccurate Customer Information
Criticality: High
PossibleDamage: Regulatory fines, financial losses, and reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Customer service disruptions, compliance violations, and loss of customer trust
RiskDescription: Failure to review and update customer information may result in inaccurate records, le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated alerts for outdated information", "2": "Provide regular trainin
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 402:
RiskId: 2271
ComplianceId: 2933
RiskTitle: Identity Fraud Risk
Criticality: High
PossibleDamage: Identity theft, financial fraud, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of customer trust, legal implications, financial losses
RiskDescription: Failure to verify customer identification documents may result in fraudulent activities a

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust document verification procedures", "2": "Regularly update staff
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 403:
RiskId: 2272
ComplianceId: 2934
RiskTitle: Outdated Customer Information Risk
Criticality: Medium
PossibleDamage: Increased fraud risk, regulatory non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: Increased fraud incidents, regulatory penalties, reputational harm
RiskDescription: Failure to update customer identification information annually may result in outdated r
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate customer identification review processes", "2": "Implement strict penalti
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 404:
RiskId: 2273

ComplianceId: 2935
RiskTitle: Inadequate Due Diligence Practices by Introducers
Criticality: High
PossibleDamage: Potential regulatory violations, exposure to high-risk entities, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Increased compliance risk and potential financial penalties
RiskDescription: Failure to implement the due diligence checklist may result in inadequate assessment
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for compliance teams on checklist implementation", "2":
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 405:
RiskId: 2274
ComplianceId: 2936
RiskTitle: Outdated Due Diligence Assessments on Introducers
Criticality: Medium
PossibleDamage: Exposure to risks associated with non-compliant introducers, potential regulatory vio
Category: Operational
RiskType: Inherent
BusinessImpact: Increased compliance risk and potential operational disruptions
RiskDescription: Failure to review due diligence practices periodically may result in outdated assessme
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Automate reminders for biennial reviews", "2": "Establish clear review criteria and

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 406:

RiskId: 2275

ComplianceId: 2937

RiskTitle: Non-compliance with AML/CFT Training Requirements

Criticality: High

PossibleDamage: Potential regulatory fines and reputational damage.

Category: Compliance

RiskType: Current

BusinessImpact: All business units

RiskDescription: Failure to comply with ongoing training requirements may result in employees not und

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update training content based on regulatory changes", "2": "Provide refr

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 407:

RiskId: 2276

ComplianceId: 2938

RiskTitle: Non-compliance with Regulatory Update Training

Criticality: Medium

PossibleDamage: Penalties for non-compliance with new regulations.

Category: Compliance
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to conduct training on regulatory updates may result in employees not being a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a process to quickly disseminate regulatory updates to employees", "2":
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 408:
RiskId: 2277
ComplianceId: 2939
RiskTitle: Inadequate Understanding of AML/CFT Regulations
Criticality: High
PossibleDamage: Increased risk of money laundering and terrorist financing activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, reputational damage, and legal consequences
RiskDescription: Employees lacking understanding of AML/CFT regulations may inadvertently facilitate
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance training materials and methods to improve understanding", "2": "Provide
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 409:
RiskId: 2278
ComplianceId: 2940
RiskTitle: False Customer Identification
Criticality: High
PossibleDamage: Facilitation of money laundering or terrorist financing activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal and reputational damage
RiskDescription: Customers providing false identification documents may lead to DNFBPs unknowingly
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance customer due diligence procedures", "2": "Implement electronic verificat
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 410:
RiskId: 2279
ComplianceId: 2941
RiskTitle: Inconsistent Document Verification
Criticality: Medium
PossibleDamage: Regulatory non-compliance
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential fines and sanctions
RiskDescription: Accepting invalid or incorrect identification documents may result in regulatory scrutin

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update the checklist of acceptable documents", "2": "Provide ongoing tr
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 411:
RiskId: 2280
ComplianceId: 2942
RiskTitle: Unidentified Beneficial Owners
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal actions
Category: Compliance
RiskType: Current
BusinessImpact: Non-compliance may lead to financial penalties and loss of reputation.
RiskDescription: Failure to collect ownership structure documentation may result in unidentified benefic
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for compliance teams on documentation requirements", "2": "Aut
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 412:
RiskId: 2281

ComplianceId: 2943
RiskTitle: Inaccurate Beneficial Ownership Verification
Criticality: High
PossibleDamage: Legal actions, financial penalties, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Non-compliance may lead to severe financial and reputational consequences.
RiskDescription: Failure to accurately verify beneficial ownership information may result in compliance
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Utilize multiple verification sources for cross-validation", "2": "Implement regular a
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 413:
RiskId: 2282
ComplianceId: 2944
RiskTitle: Misuse of Business Relationship Information
Criticality: High
PossibleDamage: Legal implications, loss of trust with customers
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of business, reputational damage
RiskDescription: Failure to collect accurate information about business relationships may lead to misur
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training and updates for relationship managers", "2": "Implement automat

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 414:

RiskId: 2283

ComplianceId: 2945

RiskTitle: Failure to Detect Suspicious Transactions

Criticality: High

PossibleDamage: Regulatory fines, reputational damage, and legal actions

Category: Operational

RiskType: Current

BusinessImpact: Loss of credibility, financial penalties, and potential legal consequences

RiskDescription: Undetected suspicious transactions can lead to severe consequences for the DNFBP

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training for compliance analysts on using the monitoring software", "2": "F

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 415:

RiskId: 2284

ComplianceId: 2946

RiskTitle: Inadequate Transaction Monitoring

Criticality: Medium

PossibleDamage: Missed suspicious transactions and regulatory non-compliance

Category: Operational
RiskType: Current
BusinessImpact: Potential regulatory fines, reputational damage, and increased scrutiny
RiskDescription: Failure to continuously monitor transactions and conduct timely reviews may lead to n
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear review schedules and escalation procedures for flagged transactio
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 416:
RiskId: 2285
ComplianceId: 2947
RiskTitle: Failure to Identify Beneficial Owners
Criticality: High
PossibleDamage: Potential involvement in money laundering or terrorist financing activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Legal and financial penalties, loss of reputation, and regulatory sanctions
RiskDescription: Failure to identify beneficial owners could result in DNFBPs unknowingly facilitating ill
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures for beneficial owners", "2": "Implement ongoin
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 417:
RiskId: 2286
ComplianceId: 2948
RiskTitle: Failure to Identify PEPs
Criticality: High
PossibleDamage: Facilitation of money laundering or terrorist financing activities
Category: Compliance
RiskType: Current
BusinessImpact: Compliance penalties, reputational damage, legal consequences
RiskDescription: Failure to identify and monitor PEPs may result in the DNFBP unknowingly facilitating
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence procedures for high-risk customers", "2": "Regular review
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 418:
RiskId: 2287
ComplianceId: 2949
RiskTitle: Outdated PEP Information
Criticality: Medium
PossibleDamage: Increased risk exposure
Category: Compliance
RiskType: Current
BusinessImpact: Compliance penalties, reputational damage, legal consequences
RiskDescription: Failure to conduct annual reviews of PEP information may result in outdated profiles,

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated reminders for annual PEP reviews", "2": "Regular training on PEP iden
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 419:
RiskId: 2288
ComplianceId: 2950
RiskTitle: Failure to Conduct Risk Assessment
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, increased exposure to financial crimes
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial losses, reputational harm
RiskDescription: Failure to conduct risk assessments may result in non-compliance with AML regulatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust KYC procedures", "2": "Provide ongoing training to risk manage
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 420:
RiskId: 2289

ComplianceId: 2951
RiskTitle: Lack of Senior Management Approval Documentation
Criticality: High
PossibleDamage: Non-compliance with AML/CFT guidelines and potential regulatory penalties
Category: Compliance
RiskType: Residual
BusinessImpact: Potential fines, reputational damage, and increased regulatory scrutiny
RiskDescription: Failure to document senior management approvals for PEP relationships may result i
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a standardized documentation process", "2": "Provide training on docu
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 421:
RiskId: 2290
ComplianceId: 2952
RiskTitle: Lack of Senior Management Approval Reporting
Criticality: High
PossibleDamage: Non-compliance with AML/CFT guidelines and potential regulatory sanctions
Category: Compliance
RiskType: Residual
BusinessImpact: Potential fines, reputational damage, and increased regulatory scrutiny
RiskDescription: Failure to report senior management approvals for PEP relationships may result in re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish reporting schedule", "2": "Implement review process for accuracy", "3": "

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 422:

RiskId: 2291

ComplianceId: 2953

RiskTitle: Failure to Detect Suspicious PEP Transactions

Criticality: High

PossibleDamage: Regulatory fines, reputational damage, legal implications

Category: Compliance

RiskType: Current

BusinessImpact: Compliance, Legal

RiskDescription: Failure to detect suspicious PEP transactions could lead to severe regulatory conseq

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhance transaction monitoring systems", "2": "Provide regular training to staff or

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 423:

RiskId: 2292

ComplianceId: 2954

RiskTitle: Outdated Customer Information

Criticality: Medium

PossibleDamage: Ineffective monitoring, increased risk of financial crimes

Category: Operational
RiskType: Current
BusinessImpact: AML/CFT, Compliance
RiskDescription: Outdated or inaccurate customer information could compromise the effectiveness of r
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement regular customer information update procedures", "2": "Conduct period
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 424:
RiskId: 2293
ComplianceId: 2955
RiskTitle: Failure to Verify Source of Wealth and Funds for PEPs
Criticality: High
PossibleDamage: Potential money laundering or terrorist financing activities going undetected
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Failure to verify the source of wealth and funds for PEPs may result in unknowingly fa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence for high-risk PEPs", "2": "Regular training for compliance
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 425:
RiskId: 2294
ComplianceId: 2956
RiskTitle: Misrepresentation of PEP Influence
Criticality: High
PossibleDamage: Regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory scrutiny and fines
RiskDescription: Misrepresentation of a PEP's influence can lead to regulatory violations and reputatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify information with official sources", "2": "Cross-check data with other complia
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 426:
RiskId: 2295
ComplianceId: 2957
RiskTitle: Undisclosed Conflicts of Interest
Criticality: Medium
PossibleDamage: Conflicts impacting business decisions
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential conflicts leading to biased decisions
RiskDescription: Undisclosed relationships with family members or associates can lead to conflicts of i

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Require PEPs to disclose all family relationships", "2": "Conduct periodic reviews
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 427:
RiskId: 2296
ComplianceId: 2958
RiskTitle: Risk of Money Laundering and Financial Crimes
Criticality: High
PossibleDamage: Potential involvement in illegal activities and severe financial penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Severe financial and reputational damage
RiskDescription: Failure to verify the source of funds and wealth for PEPs may lead to the facilitation o
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence procedures for high-risk PEPs", "2": "Utilize third-party ve
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 428:
RiskId: 2297

ComplianceId: 2959
RiskTitle: Failure to Identify Negative News on PEPs
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, and increased risk of financial crimes
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory sanctions, loss of customer trust, and financial losses
RiskDescription: Not screening PEPs for negative news may expose the organization to compliance vi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated screening tools", "2": "Regularly update screening databas
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 429:
RiskId: 2298
ComplianceId: 2960
RiskTitle: Missed Adverse Media Updates on PEPs
Criticality: Medium
PossibleDamage: Increased risk exposure, potential compliance breaches, and regulatory scrutiny
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, reputational damage, and loss of customer trust
RiskDescription: Failure to conduct periodic screening on PEPs may result in missed adverse media u
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Set up automated alerts for negative news updates", "2": "Regularly review and u
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 430:
RiskId: 2299
ComplianceId: 2961
RiskTitle: Non-Compliance with PEP Approval Requirements
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, legal actions
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal and financial consequences for the organization
RiskDescription: Failure to obtain senior management approval for PEP relationships may result in viol
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated approval workflows for PEP relationships", "2": "Conduct re
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 431:
RiskId: 2300
ComplianceId: 2962
RiskTitle: Failure to Detect Suspicious Activities in PEP Accounts
Criticality: High
PossibleDamage: Potential money laundering or terrorist financing activities going undetected

Category: Operational
RiskType: Current
BusinessImpact: Could result in regulatory fines, reputational damage, and legal actions
RiskDescription: Failure to detect suspicious activities in PEP accounts could lead to severe conseque
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for compliance monitoring teams on using automated monitoring
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 432:
RiskId: 2301
ComplianceId: 2963
RiskTitle: Ineffectiveness of Enhanced Monitoring Procedures
Criticality: Medium
PossibleDamage: Undetected suspicious activities in PEP accounts
Category: Operational
RiskType: Current
BusinessImpact: Could result in regulatory violations and reputational damage
RiskDescription: Ineffective monitoring procedures could lead to undetected suspicious activities in PE
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing key performance indicators (KPIs) for monitoring effectiveness", "2":
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 433:
RiskId: 2302
ComplianceId: 2964
RiskTitle: Outdated Due Diligence Information
Criticality: High
PossibleDamage: Increased regulatory fines and reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Non-compliance with regulatory requirements and potential loss of business opportun
RiskDescription: Failure to update due diligence information can lead to inaccurate risk assessments a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for compliance officers on PEP account reviews", "2": "Automate
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 434:
RiskId: 2303
ComplianceId: 2965
RiskTitle: Lack of Employee Awareness on PEP Risks
Criticality: High
PossibleDamage: Potential regulatory fines, reputational damage, and legal consequences
Category: Operational
RiskType: Inherent
BusinessImpact: Potential legal liabilities and damage to the organization's reputation
RiskDescription: Employees may unknowingly engage with PEPs, leading to violations of anti-money la

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update training modules to reflect current PEP risk landscape", "2": "Co
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 435:
RiskId: 2304
ComplianceId: 2966
RiskTitle: Outdated Employee Knowledge on PEP Risks
Criticality: Medium
PossibleDamage: Increased risk of compliance breaches and regulatory violations
Category: Operational
RiskType: Inherent
BusinessImpact: Potential compliance penalties and reputational damage
RiskDescription: Employees may not be aware of updated PEP risk profiles, leading to inadvertent viol
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Schedule workshops well in advance to ensure maximum participation", "2": "Inclu
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 436:
RiskId: 2305

ComplianceId: 2967
RiskTitle: Failure to Collect Identification Documents
Criticality: High
PossibleDamage: Unauthorized transactions, money laundering, regulatory fines
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial loss, reputational damage
RiskDescription: Failure to collect required identification documents may result in unauthorized transac
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for staff on document collection procedures", "2": "Imple
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 437:
RiskId: 2306
ComplianceId: 2968
RiskTitle: Failure to Verify Customer Identities
Criticality: High
PossibleDamage: Identity theft, fraudulent transactions, regulatory fines
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial loss, reputational damage
RiskDescription: Failure to verify customer identities may result in fraudulent activities, identity theft, ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implementation of biometric verification tools for enhanced security", "2": "Regula

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 438:

RiskId: 2307

ComplianceId: 2969

RiskTitle: Inaccurate Customer Risk Assessment

Criticality: High

PossibleDamage: Potential money laundering, fraud, or regulatory fines

Category: Compliance

RiskType: Inherent

BusinessImpact: Financial losses, reputational damage, regulatory penalties

RiskDescription: Failure to accurately assess customer risk may lead to the organization unknowingly f

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement a robust risk scoring system", "2": "Regularly review and update risk as

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 439:

RiskId: 2308

ComplianceId: 2970

RiskTitle: Failure to Verify Customer Identity

Criticality: High

PossibleDamage: Unauthorized transactions, money laundering, terrorist financing

Category: Operational
RiskType: Current
BusinessImpact: Financial loss, reputation damage, regulatory fines
RiskDescription: Failure to verify customer identity may lead to fraudulent activities and non-complianc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced customer due diligence procedures", "2": "Implement biometric verifica
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 440:
RiskId: 2309
ComplianceId: 2971
RiskTitle: Undetected Suspicious Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal consequences
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, financial losses, regulatory scrutiny
RiskDescription: Failure to monitor customer transactions may lead to undetected suspicious activities
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust transaction monitoring systems", "2": "Provide regular training t
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 441:
RiskId: 2310
ComplianceId: 2972
RiskTitle: Failure to Report Suspicious Activities
Criticality: High
PossibleDamage: Regulatory sanctions, legal actions, reputational harm
Category: Operational
RiskType: Inherent
BusinessImpact: Legal consequences, reputational damage, financial losses
RiskDescription: Not reporting suspicious activities may result in regulatory non-compliance, legal actio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting procedures", "2": "Provide training on identifying and rep
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 442:
RiskId: 2311
ComplianceId: 2973
RiskTitle: Failure to Conduct Enhanced Due Diligence Verification
Criticality: High
PossibleDamage: Increased exposure to financial crimes and regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, reputational damage, and legal consequences
RiskDescription: Failure to conduct enhanced due diligence verification may lead to unknowingly enga

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated verification tools", "2": "Enhance training for compliance off
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 443:
RiskId: 2312
ComplianceId: 2974
RiskTitle: Inadequate Risk Assessment for High-Risk Customers
Criticality: Medium
PossibleDamage: Exposure to financial crimes, regulatory violations, and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, reputational damage, and legal consequences
RiskDescription: Inadequate risk assessments may result in unknowingly engaging with high-risk custo
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement risk-based customer due diligence procedures", "2": "Utilize advanced
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 444:
RiskId: 2313

ComplianceId: 2975
RiskTitle: Loss of Customer Due Diligence Records
Criticality: High
PossibleDamage: Loss of critical customer data, regulatory fines, legal actions
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of customer onboarding processes, potential legal consequences
RiskDescription: Loss of customer due diligence records due to system failure or unauthorized access
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular data backups and offsite storage", "2": "Implement access controls and e
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 445:
RiskId: 2314
ComplianceId: 2976
RiskTitle: Failure to Identify High-Risk Customers
Criticality: High
PossibleDamage: Increased exposure to money laundering or terrorist financing activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance, Legal, Reputational
RiskDescription: Failure to properly identify high-risk customers can result in facilitating money launder
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement enhanced due diligence procedures for high-risk customers", "2": "Reg

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 446:

RiskId: 2315

ComplianceId: 2977

RiskTitle: Failure to Conduct Enhanced Due Diligence

Criticality: High

PossibleDamage: Increased exposure to financial crimes and regulatory penalties

Category: Compliance

RiskType: Inherent

BusinessImpact: Financial losses, regulatory fines, and reputational damage

RiskDescription: Failure to conduct Enhanced Due Diligence may result in unknowingly engaging with

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhanced staff training on EDD procedures", "2": "Regular audits of EDD process

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 447:

RiskId: 2316

ComplianceId: 2978

RiskTitle: Outdated Enhanced Due Diligence Procedures

Criticality: Medium

PossibleDamage: Outdated or ineffective EDD procedures leading to compliance breaches

Category: Compliance
RiskType: Inherent
BusinessImpact: Operational disruptions, regulatory fines, and reputational harm
RiskDescription: Failure to review and update EDD procedures may result in ineffective risk assessme
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular updates to EDD protocols", "2": "Continuous monitoring of regulatory cha
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 448:
RiskId: 2317
ComplianceId: 2979
RiskTitle: Non-Compliance with AML/CFT Regulations
Criticality: High
PossibleDamage: Legal penalties, fines, and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units involved in customer onboarding and due diligence processes
RiskDescription: Failure to comply with AML/CFT regulations can result in severe legal and reputationa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions", "2": "Strict enforcement of attendance", "3": "Consequ
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 449:
RiskId: 2318
ComplianceId: 2980
RiskTitle: False Identity Risk
Criticality: High
PossibleDamage: Legal penalties, loss of reputation, and financial losses due to fraudulent activities.
Category: Operational
RiskType: Current
BusinessImpact: Non-compliance with identity verification procedures may result in regulatory fines, le
RiskDescription: Customers providing false identities may use the organization's services for illicit purp
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated verification tools for efficient and accurate identity checks",
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 450:
RiskId: 2319
ComplianceId: 2981
RiskTitle: Failure to Verify Beneficial Ownership
Criticality: High
PossibleDamage: Potential involvement in money laundering activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance, Legal
RiskDescription: Failure to verify beneficial ownership may result in non-compliance with AML/CFT reg

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust customer due diligence procedures", "2": "Regularly update ow
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 451:
RiskId: 2320
ComplianceId: 2982
RiskTitle: Undetected Suspicious Activities
Criticality: High
PossibleDamage: Financial penalties, reputational damage, regulatory sanctions
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of customer trust, regulatory fines, legal implications
RiskDescription: Failure to detect and report suspicious activities can result in severe financial and rep
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance transaction monitoring systems with advanced analytics and machine le
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 452:
RiskId: 2321

ComplianceId: 2983
RiskTitle: Delayed Reporting of Suspicious Activities
Criticality: High
PossibleDamage: Regulatory fines, legal implications, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, loss of credibility, financial penalties
RiskDescription: Failure to report suspicious activities immediately may lead to regulatory violations an
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish automated reporting triggers for suspicious activities", "2": "Conduct reg
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 453:
RiskId: 2322
ComplianceId: 2984
RiskTitle: Failure to Identify and Verify High-Risk Customers
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, increased risk of financial crime
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal and financial consequences, damage to reputation
RiskDescription: Failure to identify and verify high-risk customers may lead to the organization unknow
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Enhance customer due diligence processes", "2": "Implement transaction monitor
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 454:
RiskId: 2323
ComplianceId: 2985
RiskTitle: Failure to Detect High-Risk Transactions
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal and financial liabilities, damage to reputation
RiskDescription: Inadequate monitoring of high-risk transactions may result in regulatory non-complian
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced training for compliance monitoring team", "2": "Regular audits of monito
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 455:
RiskId: 2324
ComplianceId: 2986
RiskTitle: Failure to Document Senior Management Approval
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, and loss of business opportunities.

Category: Compliance
RiskType: Inherent
BusinessImpact: Potential financial losses and damage to the organization's reputation.
RiskDescription: Lack of documented senior management approval may lead to non-compliance with r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear documentation procedures", "2": "Regularly review and update ap
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 456:
RiskId: 2325
ComplianceId: 2987
RiskTitle: Lack of Senior Management Approval for High-Risk Relationships
Criticality: Critical
PossibleDamage: Financial crime exposure, regulatory violations, and reputational harm.
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, legal actions, and damage to the organization's reputation.
RiskDescription: Engaging in high-risk relationships without senior management approval may lead to
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear approval guidelines and responsibilities", "2": "Provide regular trai
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 457:
RiskId: 2326
ComplianceId: 2988
RiskTitle: Unidentified Beneficial Owners
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, and legal actions.
Category: Compliance
RiskType: Current
BusinessImpact: Legal and financial implications for the organization.
RiskDescription: Failure to identify beneficial owners can lead to potential money laundering or terroris
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for compliance officers on the cascade methodology", "
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 458:
RiskId: 2327
ComplianceId: 2989
RiskTitle: Failure to Verify Ownership
Criticality: High
PossibleDamage: Involvement in illicit activities
Category: Compliance
RiskType: Current
BusinessImpact: Legal and financial consequences
RiskDescription: Non-compliance with ownership verification requirements may result in DNFBPs unwi

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust customer due diligence procedures", "2": "Regularly update ow
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 459:
RiskId: 2328
ComplianceId: 2990
RiskTitle: Failure to Verify Control
Criticality: High
PossibleDamage: Regulatory sanctions and reputational harm
Category: Compliance
RiskType: Current
BusinessImpact: Financial and reputational consequences
RiskDescription: Non-compliance with control verification requirements may lead to regulatory penaltie
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust customer due diligence procedures", "2": "Regularly update cor
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 460:
RiskId: 2329

ComplianceId: 2991
RiskTitle: Failure to Verify Client Identity
Criticality: High
PossibleDamage: Potential money laundering, fraud, or terrorist financing activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny and potential fines
RiskDescription: Failure to verify client identity may result in DNFBPs unknowingly facilitating illicit acti
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures for intermediary clients", "2": "Implement trans
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 461:
RiskId: 2330
ComplianceId: 2992
RiskTitle: Failure to Conduct Transaction Risk Assessments
Criticality: Medium
PossibleDamage: Facilitating illicit activities or financial losses
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory violations and financial losses
RiskDescription: Failure to assess transaction risks may result in DNFBPs unknowingly facilitating high
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Enhance transaction monitoring capabilities", "2": "Implement real-time transactio

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 462:

RiskId: 2331

ComplianceId: 2993

RiskTitle: Non-compliance with Identification and Verification Requirements

Criticality: High

PossibleDamage: Regulatory penalties, reputational damage, and loss of client trust

Category: Compliance

RiskType: Current

BusinessImpact: Potential fines, legal actions, and damage to reputation

RiskDescription: Failure to verify beneficial owners in pooled accounts may lead to non-compliance wit

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear identification and verification procedures", "2": "Regular training fo

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 463:

RiskId: 2332

ComplianceId: 2994

RiskTitle: Failure to Verify High-Risk Accounts

Criticality: Medium

PossibleDamage: Financial losses, regulatory fines, and reputational harm

Category: Operational
RiskType: Current
BusinessImpact: Increased exposure to money laundering and fraudulent activities
RiskDescription: Neglecting to verify high-risk accounts may expose the organization to financial and re
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enhance due diligence procedures for high-risk clients", "2": "Implement automate
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 464:
RiskId: 2333
ComplianceId: 2995
RiskTitle: Failure to Develop Customer Acceptance Policy
Criticality: High
PossibleDamage: Onboarding high-risk customers without appropriate monitoring
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance Officer and Risk Management Team
RiskDescription: Failure to develop the policy may result in onboarding high-risk customers without app
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Utilize risk assessment tools and guidelines from the Financial Intelligence Author
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 465:
RiskId: 2334
ComplianceId: 2996
RiskTitle: Failure to Identify High-Risk Customers
Criticality: Medium
PossibleDamage: Increased risk exposure and regulatory non-compliance
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance Officer and Risk Management Team
RiskDescription: Failure to identify high-risk customers may lead to increased risk exposure and regula
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on risk assessment tools and guidelines", "2": "Cross-verification
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 466:
RiskId: 2335
ComplianceId: 2997
RiskTitle: Inadequate EDD Procedures for High-Risk Customers
Criticality: High
PossibleDamage: Increased exposure to financial crimes and regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Customer relationships, reputation, and regulatory standing may be significantly impa
RiskDescription: Failure to implement EDD procedures for high-risk customers may lead to regulatory

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and updates on EDD procedures", "2": "Automated alerts for EDD
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 467:
RiskId: 2336
ComplianceId: 2998
RiskTitle: Outdated Risk Assessments for High-Risk Customers
Criticality: Medium
PossibleDamage: Inadequate mitigation measures and increased exposure to financial crimes
Category: Compliance
RiskType: Inherent
BusinessImpact: Customer relationships, reputation, and regulatory standing may be impacted.
RiskDescription: Failure to conduct regular reviews of high-risk customer profiles may result in outdate
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated reminders for annual reviews", "2": "Integration of risk assessment too
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 468:
RiskId: 2337

ComplianceId: 2999
RiskTitle: Undetected Suspicious Activities in High-Risk Accounts
Criticality: High
PossibleDamage: Legal penalties, reputational damage, loss of customer trust
Category: Operational
RiskType: Current
BusinessImpact: Non-compliance with AML/CFT regulations, regulatory fines, damage to reputation
RiskDescription: Failure to monitor high-risk accounts may result in undetected suspicious activities, le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated alerts for high-risk account monitoring", "2": "Enhance train
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 469:
RiskId: 2338
ComplianceId: 3000
RiskTitle: Ineffective Utilization of Transaction Monitoring Software
Criticality: Medium
PossibleDamage: Non-compliance with regulations, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Missed suspicious activities, regulatory fines, financial penalties
RiskDescription: Failure to effectively utilize transaction monitoring software may lead to missed suspic
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly update and calibrate transaction monitoring software", "2": "Conduct tra

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 470:

RiskId: 2339

ComplianceId: 3001

RiskTitle: Incomplete Originator and Beneficiary Information

Criticality: High

PossibleDamage: Processing errors, fraudulent transactions, regulatory fines

Category: Operational

RiskType: Current

BusinessImpact: Non-compliance, financial losses

RiskDescription: Failure to collect complete originator and beneficiary information may lead to processi

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training for staff on information collection procedures", "2": "Periodic audi

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 471:

RiskId: 2340

ComplianceId: 3002

RiskTitle: Failure to Monitor Wire Transfers Daily

Criticality: High

PossibleDamage: Potential fines or penalties for non-compliance

Category: Operational
RiskType: Residual
BusinessImpact: Financial losses due to regulatory fines
RiskDescription: Not monitoring wire transfers daily could result in incomplete information being reporte
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring systems", "2": "Provide regular training to staff o
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 472:
RiskId: 2341
ComplianceId: 3003
RiskTitle: Failure to Flag Incomplete Transactions
Criticality: Medium
PossibleDamage: Inaccurate reporting and regulatory issues
Category: Operational
RiskType: Residual
BusinessImpact: Potential regulatory scrutiny and operational disruptions
RiskDescription: Not flagging incomplete transactions could result in inaccurate reporting to authorities
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update and test the automated monitoring systems", "2": "Provide traini
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 473:
RiskId: 2342
ComplianceId: 3004
RiskTitle: Risk of Fraudulent Transactions
Criticality: High
PossibleDamage: Financial losses, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Customers providing incomplete information for wire transfers may lead to fraudulent
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence procedures", "2": "Additional customer training", "3": "Rel
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 474:
RiskId: 2139
ComplianceId: 2801
RiskTitle: Failure to Verify Customer Identity
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Compliance
RiskType: Current
BusinessImpact: Loss of customer trust, regulatory penalties, financial losses
RiskDescription: Failure to verify customer identities may result in unauthorized account openings, frau

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance customer identification procedures through regular training and updates
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 475:
RiskId: 2140
ComplianceId: 2802
RiskTitle: Inaccurate Customer Risk Assessment
Criticality: High
PossibleDamage: Undetected high-risk customers engaging in illicit activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Failure to accurately assess customer risk levels may result in high-risk customers en
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance customer due diligence procedures", "2": "Implement enhanced transact
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 476:
RiskId: 2141

ComplianceId: 2803
RiskTitle: Ineffective Transaction Monitoring
Criticality: Medium
PossibleDamage: Undetected suspicious transactions leading to financial crimes
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Inadequate transaction monitoring processes may result in undetected suspicious tra
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 45.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enhance transaction monitoring algorithms", "2": "Implement real-time transaction
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 477:
RiskId: 2142
ComplianceId: 2804
RiskTitle: Failure to Report Suspicious Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, increased risk of financial crimes
Category: Compliance
RiskType: Current
BusinessImpact: Potential regulatory fines, reputational damage, increased risk exposure
RiskDescription: Failure to report suspicious activities in a timely manner may lead to regulatory scrutin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on reporting procedures", "2": "Implement automated reporting to

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 478:

RiskId: 2143

ComplianceId: 2805

RiskTitle: Money Laundering Risk

Criticality: High

PossibleDamage: Financial losses, regulatory fines, reputational damage

Category: Compliance

RiskType: Inherent

BusinessImpact: Potential disruption of business operations and loss of customer trust

RiskDescription: Failure to conduct comprehensive risk assessments may lead to unidentified money l

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhance transaction monitoring capabilities", "2": "Implement enhanced customer

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 479:

RiskId: 2144

ComplianceId: 2806

RiskTitle: Failure to Collect and Verify Customer Information

Criticality: High

PossibleDamage: Increased exposure to money laundering, fraud, and regulatory fines

Category: Compliance
RiskType: Residual
BusinessImpact: Potential regulatory fines, reputational damage, loss of customer trust
RiskDescription: Failure to collect and verify customer information for high-risk customers may result in
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on enhanced due diligence procedures", "2": "Automated
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 480:
RiskId: 2145
ComplianceId: 2807
RiskTitle: Failure to Obtain Senior Management Approval
Criticality: High
PossibleDamage: Increased exposure to financial, reputational, and regulatory risks
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units within the institution may be impacted by regulatory fines, legal acti
RiskDescription: Failure to obtain senior management approval for high-risk customer relationships ma
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a clear approval process with defined criteria", "2": "Provide regular tra
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 481:
RiskId: 2146
ComplianceId: 2808
RiskTitle: Money Laundering Risk
Criticality: High
PossibleDamage: Potential regulatory fines and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Legal and financial implications
RiskDescription: Failure to accurately document client wealth sources may lead to potential money lau
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust client due diligence procedures", "2": "Enhance staff training on
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 482:
RiskId: 2147
ComplianceId: 2809
RiskTitle: Compliance Risk
Criticality: Medium
PossibleDamage: Potential regulatory non-compliance and financial penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Operational disruptions and financial losses
RiskDescription: Failure to update client wealth information regularly may result in compliance issues a

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated wealth update reminders", "2": "Enhance client communica
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 483:
RiskId: 2148
ComplianceId: 2810
RiskTitle: Failure to Detect Suspicious Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential regulatory sanctions and loss of customer trust
RiskDescription: The failure to detect suspicious transactions could result in the institution being used f
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update the monitoring system to adapt to new threats", "2": "Provide tra
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 484:
RiskId: 2149

ComplianceId: 2811
RiskTitle: Outdated or Inaccurate Client Information
Criticality: Medium
PossibleDamage: Regulatory non-compliance, increased risk of financial crimes
Category: Operational
RiskType: Current
BusinessImpact: Potential regulatory fines and loss of credibility
RiskDescription: Outdated or inaccurate client information could result in the institution unknowingly fac
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a client information verification process", "2": "Provide training to staff
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 485:
RiskId: 2150
ComplianceId: 2812
RiskTitle: Client Identification Risk
Criticality: High
PossibleDamage: Failure to identify clients accurately may result in regulatory fines and reputational da
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, loss of reputation, and legal consequences.
RiskDescription: Failure to identify clients accurately may lead to involvement in money laundering or t
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement robust client identification procedures", "2": "Regularly update client id

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 486:

RiskId: 2151

ComplianceId: 2813

RiskTitle: Annual Client Verification Risk

Criticality: Medium

PossibleDamage: Failure to update client information may result in regulatory fines and operational dis

Category: Compliance

RiskType: Inherent

BusinessImpact: Potential regulatory fines, operational disruptions, and reputational damage.

RiskDescription: Outdated client information may expose the organization to financial crimes or regulat

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement regular client verification processes", "2": "Establish clear guidelines fo

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 487:

RiskId: 2152

ComplianceId: 2814

RiskTitle: Undisclosed Illegal Financial Activities

Criticality: High

PossibleDamage: Reputational damage, regulatory fines, loss of high-net-worth clients

Category: Operational
RiskType: Current
BusinessImpact: Disruption of private banking operations and loss of client trust
RiskDescription: Failure to identify undisclosed illegal financial activities of high-net-worth clients may l
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence for high-risk clients", "2": "Regular monitoring of client tra
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 488:
RiskId: 2153
ComplianceId: 2815
RiskTitle: Undisclosed Changes in Financial Circumstances
Criticality: Medium
PossibleDamage: Increased risk exposure, regulatory non-compliance, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate risk assessment and potential financial losses
RiskDescription: Failure to review high-net-worth clients' source of wealth annually or during significant
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated annual review process", "2": "Enhanced monitoring for significant clien
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 489:
RiskId: 2154
ComplianceId: 2816
RiskTitle: Failure to Monitor High-Value Transactions
Criticality: High
PossibleDamage: Increased risk of money laundering and financial crimes
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, regulatory fines, reputational damage
RiskDescription: Failure to monitor high-value transactions may result in undetected money laundering
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated transaction monitoring systems", "2": "Conduct regular train
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 490:
RiskId: 2155
ComplianceId: 2817
RiskTitle: Delayed Detection of Suspicious Activities
Criticality: Medium
PossibleDamage: Increased exposure to money laundering risks
Category: Operational
RiskType: Inherent
BusinessImpact: Operational inefficiencies, potential regulatory issues
RiskDescription: Failure to conduct real-time monitoring and monthly reviews may lead to delayed dete

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Utilize real-time transaction monitoring systems", "2": "Establish clear procedures
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 491:
RiskId: 2156
ComplianceId: 2818
RiskTitle: Inadequate EDD Training
Criticality: High
PossibleDamage: Increased risk exposure, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, regulatory sanctions, reputational harm
RiskDescription: Failure to provide adequate EDD training may result in staff not identifying risks effect
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training completion", "2": "Provide ongoing support and res
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 492:
RiskId: 2157

ComplianceId: 2819
RiskTitle: Ineffective Training Delivery
Criticality: Medium
PossibleDamage: Staff misunderstanding EDD procedures, leading to compliance breaches
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, compliance breaches, reputational harm
RiskDescription: Failure to deliver EDD training effectively may result in staff not fully understanding pr
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular feedback and evaluation of training methods", "2": "Continuous improvem
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 493:
RiskId: 2158
ComplianceId: 2820
RiskTitle: Inadequate Risk Assessment Framework
Criticality: High
PossibleDamage: Undetected high-risk transactions and potential financial losses.
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses and reputational damage.
RiskDescription: Failure to implement a standardized risk assessment framework may result in incomp
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on the risk assessment framework", "2": "Continuous monitoring

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 494:

RiskId: 2159

ComplianceId: 2821

RiskTitle: Outdated Risk Assessments

Criticality: Medium

PossibleDamage: Increased exposure to potential risks and compliance violations.

Category: Operational

RiskType: Inherent

BusinessImpact: Financial losses and regulatory penalties.

RiskDescription: Failure to review risk assessments quarterly may result in outdated risk information ar

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear review schedule and responsibilities", "2": "Document all review fir

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 495:

RiskId: 2160

ComplianceId: 2822

RiskTitle: Undetected Compliance Issues

Criticality: High

PossibleDamage: Regulatory fines, reputational damage, increased financial crime incidents

Category: Operational
RiskType: Current
BusinessImpact: Private banking operations
RiskDescription: Failure to conduct audits may result in undetected compliance issues, leading to regu
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust audit schedule and allocate resources accordingly", "2": "Prov
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 496:
RiskId: 2161
ComplianceId: 2823
RiskTitle: Inadequate Response to Emerging Risks
Criticality: Medium
PossibleDamage: Regulatory non-compliance, increased financial crime risks
Category: Operational
RiskType: Current
BusinessImpact: Private banking operations
RiskDescription: Failure to conduct triggered audits may result in inadequate response to emerging ris
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear criteria for triggering additional audits", "2": "Regularly monitor cha
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 497:
RiskId: 2162
ComplianceId: 2824
RiskTitle: Increased Exposure to Financial Crimes
Criticality: High
PossibleDamage: Financial penalties, legal actions, reputational harm
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, loss of customer trust
RiskDescription: Failure to conduct comprehensive risk assessments for high-risk customers may resu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance customer due diligence procedures for high-risk customers", "2": "Imple
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 498:
RiskId: 2163
ComplianceId: 2825
RiskTitle: Inadequate EDD Training
Criticality: High
PossibleDamage: Inadequate risk identification and management, potential regulatory fines or reputati
Category: Operational
RiskType: Current
BusinessImpact: Compliance, Legal, Financial
RiskDescription: Failure to comply with EDD training requirements may result in staff being ill-equippe

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update training materials to reflect current regulations and risks", "2": "F
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 499:
RiskId: 2164
ComplianceId: 2826
RiskTitle: Incomplete Online EDD Training
Criticality: Medium
PossibleDamage: Gaps in knowledge and understanding of EDD principles, potential errors in risk ass
Category: Operational
RiskType: Current
BusinessImpact: Compliance, Legal
RiskDescription: Failure to complete online training modules may result in staff having incomplete knov
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Monitor completion rates and follow up with staff who have not completed the mo
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 500:
RiskId: 2165

ComplianceId: 2827
RiskTitle: Non-Compliance with EDD Audit Requirements
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, increased risk exposure
Category: Compliance
RiskType: Inherent
BusinessImpact: Non-compliance may lead to regulatory penalties and reputational harm.
RiskDescription: Failure to conduct audits may result in ineffective risk management and non-complian
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated audit scheduling system", "2": "Provide regular training to a
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 501:
RiskId: 2166
ComplianceId: 2828
RiskTitle: Delayed Response to Significant Findings
Criticality: Medium
PossibleDamage: Increased risk exposure, non-compliance, reputational harm
Category: Compliance
RiskType: Inherent
BusinessImpact: Failure to address significant findings promptly may result in increased risk exposure
RiskDescription: Delayed response to significant findings may lead to ineffective risk management and
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear escalation procedures for audit findings", "2": "Implement regular r

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 502:

RiskId: 2167

ComplianceId: 2829

RiskTitle: Failure to Conduct Annual Risk Assessment

Criticality: High

PossibleDamage: Increased exposure to ML/TF risks and regulatory penalties

Category: Compliance

RiskType: Current

BusinessImpact: Regulatory fines and reputational damage

RiskDescription: Not conducting annual risk assessments may lead to unidentified risks and non-comp

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on risk assessment procedures", "2": "Engage external auditors f

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 503:

RiskId: 2168

ComplianceId: 2830

RiskTitle: Money Laundering Risk

Criticality: High

PossibleDamage: Legal and financial penalties, reputational damage

Category: Compliance
RiskType: Current
BusinessImpact: Increased scrutiny from regulators, loss of customer trust
RiskDescription: Failure to conduct proper due diligence could result in the business unknowingly facili
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance customer due diligence procedures", "2": "Implement transaction monito
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 504:
RiskId: 2169
ComplianceId: 2831
RiskTitle: Transaction Monitoring Failure
Criticality: Medium
PossibleDamage: Regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Increased regulatory oversight, loss of customer trust
RiskDescription: Failure to detect suspicious transactions could result in the business unknowingly faci
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enhance transaction monitoring algorithms", "2": "Implement real-time transaction
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 505:
RiskId: 2170
ComplianceId: 2832
RiskTitle: Inaccurate Client Net Worth Reporting
Criticality: High
PossibleDamage: Misguided financial planning, increased risk exposure, regulatory fines.
Category: Operational
RiskType: Residual
BusinessImpact: Impaired decision-making, financial losses, reputational damage.
RiskDescription: Failure to accurately document client net worth may result in incorrect financial advice
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated data validation tools", "2": "Provide training to staff on prop
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 506:
RiskId: 2171
ComplianceId: 2833
RiskTitle: Unverified Source of Wealth
Criticality: High
PossibleDamage: Money laundering, fraud, regulatory fines, reputational damage.
Category: Legal
RiskType: Residual
BusinessImpact: Legal consequences, financial losses, reputational harm.
RiskDescription: Failure to verify clients' declared source of wealth may result in facilitating illegal activ

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct background checks on clients", "2": "Require supporting documentation f
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 507:
RiskId: 2172
ComplianceId: 2834
RiskTitle: Failure to Verify Source of Wealth Documentation
Criticality: High
PossibleDamage: Potential money laundering activities going undetected
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial penalties, reputational damage
RiskDescription: Failure to verify the legitimacy of source of wealth documentation may result in the ins
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance document verification processes", "2": "Implement regular audits of sour
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 508:
RiskId: 2173

ComplianceId: 2835
RiskTitle: Failure to Verify Source of Wealth for Significant Transactions
Criticality: High
PossibleDamage: Potential money laundering activities going undetected
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial penalties, reputational damage
RiskDescription: Failure to verify the legitimacy of source of wealth for significant transactions may resu
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 62.05
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance transaction monitoring processes", "2": "Implement regular audits of sign
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 509:
RiskId: 2174
ComplianceId: 2836
RiskTitle: Inaccurate Customer Risk Assessment
Criticality: High
PossibleDamage: Potential exposure to high-risk customers
Category: Operational
RiskType: Inherent
BusinessImpact: Increased compliance and regulatory scrutiny, reputational damage
RiskDescription: Failure to accurately assess customer risk levels may result in onboarding high-risk cu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhanced training on risk assessment", "2": "Regular review of high-risk accounts

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 510:

RiskId: 2175

ComplianceId: 2837

RiskTitle: Failure to Detect Suspicious Activities

Criticality: High

PossibleDamage: Potential regulatory fines, reputational damage, legal actions

Category: Operational

RiskType: Residual

BusinessImpact: Increased compliance costs, loss of customer trust

RiskDescription: Undetected suspicious activities can lead to severe financial and reputational conseq

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enhance transaction monitoring algorithms", "2": "Implement real-time alerting me

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 511:

RiskId: 2176

ComplianceId: 2838

RiskTitle: Delayed Reporting of Suspicious Activities

Criticality: Medium

PossibleDamage: Regulatory fines, reputational damage, legal actions

Category: Operational
RiskType: Residual
BusinessImpact: Increased compliance costs, regulatory scrutiny
RiskDescription: Failure to escalate concerns related to suspicious activities in a timely manner can lea
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate escalation alerts", "2": "Implement escalation tracking system", "3": "En
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 512:
RiskId: 2177
ComplianceId: 2839
RiskTitle: Inadequate EDD and AML Training
Criticality: High
PossibleDamage: Increased risk of regulatory violations, financial losses, and reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Lack of regular training may lead to staff incompetence in identifying suspicious activi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance training content to include real-life case studies", "2": "Provide refresher
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 513:
RiskId: 2178
ComplianceId: 2840
RiskTitle: Inadequate New Staff Onboarding Training
Criticality: Medium
PossibleDamage: Early exposure to compliance risks, potential regulatory violations
Category: Compliance
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Insufficient training for new staff may lead to gaps in compliance knowledge, increasi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a structured onboarding program with clear learning objectives", "2": "
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 514:
RiskId: 2179
ComplianceId: 2841
RiskTitle: Failure to Verify Customer Identity
Criticality: High
PossibleDamage: Risk of financial fraud and money laundering
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance department
RiskDescription: Failure to verify customer identity may result in facilitating illegal activities through the

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on identification procedures", "2": "Implement automated
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 515:
RiskId: 2180
ComplianceId: 2842
RiskTitle: Outdated Customer Profiles
Criticality: Medium
PossibleDamage: Risk of facilitating money laundering
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance department
RiskDescription: Outdated customer profiles may result in the financial institution unknowingly facilitati
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate customer profile review process", "2": "Implement alert system for signi
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 516:
RiskId: 2181

ComplianceId: 2843
RiskTitle: Failure to Detect Money Laundering
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Legal and financial consequences
RiskDescription: Failure to detect money laundering activities can result in severe financial and reputat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced transaction monitoring systems", "2": "Regular staff training on money
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 517:
RiskId: 2182
ComplianceId: 2844
RiskTitle: Inaccurate Customer Risk Assessments
Criticality: Medium
PossibleDamage: Increased exposure to financial crimes, regulatory fines
Category: Compliance
RiskType: Residual
BusinessImpact: Legal and financial consequences
RiskDescription: Inaccurate customer risk assessments can lead to regulatory non-compliance and inc
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Automated alerts for profile changes", "2": "Enhanced due diligence for discrepan
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 518:
RiskId: 2183
ComplianceId: 2845
RiskTitle: Failure to Identify Beneficial Owners
Criticality: High
PossibleDamage: Increased risk of money laundering and regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Potential legal and financial penalties
RiskDescription: Failure to identify beneficial owners can lead to regulatory non-compliance and expos
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence procedures", "2": "Regular audits of ownership informatio
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 519:
RiskId: 2184
ComplianceId: 2846
RiskTitle: Insufficient Ownership Documentation
Criticality: Medium
PossibleDamage: Misinterpretation of ownership structures and legal disputes

Category: Legal
RiskType: Current
BusinessImpact: Legal disputes and potential financial losses
RiskDescription: Lack of detailed ownership documentation can lead to misunderstandings and dispute
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear documentation requirements", "2": "Regularly review and update d
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 520:
RiskId: 2185
ComplianceId: 2847
RiskTitle: Outdated Risk Assessment
Criticality: High
PossibleDamage: Misalignment with risk appetite and regulatory requirements, increased exposure to
Category: Operational
RiskType: Residual
BusinessImpact: Increased exposure to financial crimes, regulatory fines, and reputational damage
RiskDescription: Failure to conduct the annual review of the risk assessment may result in an outdated
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and updates on risk assessment methodologies", "2": "Engagem
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 521:
RiskId: 2186
ComplianceId: 2848
RiskTitle: Inadequate Customer Due Diligence
Criticality: High
PossibleDamage: Potential regulatory fines, reputational damage, and financial losses
Category: Compliance
RiskType: Residual
BusinessImpact: Non-compliance with regulatory requirements, legal implications, financial penalties
RiskDescription: Failure to adequately assess customer risk profiles and monitor transactions may lead
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance customer due diligence procedures", "2": "Implement transaction monito
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 522:
RiskId: 2187
ComplianceId: 2849
RiskTitle: Ineffective Transaction Monitoring
Criticality: High
PossibleDamage: Potential regulatory fines, reputational damage, and financial losses
Category: Compliance
RiskType: Residual
BusinessImpact: Non-compliance with regulatory requirements, legal implications, financial penalties
RiskDescription: Failure to effectively monitor transactions and detect suspicious activities may lead to

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance transaction monitoring systems", "2": "Implement automated alerts for su
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 523:
RiskId: 2188
ComplianceId: 2850
RiskTitle: Inadequate Training
Criticality: High
PossibleDamage: Increased risk of regulatory non-compliance and potential involvement in money lau
Category: Compliance
RiskType: Residual
BusinessImpact: Potential fines, reputational damage, and legal consequences
RiskDescription: Staff lacking necessary skills and knowledge may overlook red flags in customer profi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update training materials to reflect current regulations and best practice
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 524:
RiskId: 2189

ComplianceId: 2851
RiskTitle: Inaccurate Customer Profiles
Criticality: High
PossibleDamage: Inadequate risk assessment and potential exposure to financial crimes
Category: Operational
RiskType: Residual
BusinessImpact: Regulatory penalties and reputational damage
RiskDescription: Outdated or incomplete customer profiles may lead to inaccurate risk assessments, ir
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on customer profile maintenance procedures", "2": "Automated a
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 525:
RiskId: 2190
ComplianceId: 2852
RiskTitle: Missing Audit Findings
Criticality: Medium
PossibleDamage: Repeated compliance issues and inability to demonstrate remediation efforts
Category: Operational
RiskType: Residual
BusinessImpact: Regulatory fines and reputational damage
RiskDescription: Lack of documented audit findings may result in recurring compliance issues, leading
RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Centralized audit findings repository", "2": "Regular review of audit findings for co

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 526:

RiskId: 2191

ComplianceId: 2853

RiskTitle: Failure to Detect Suspicious Activities

Criticality: High

PossibleDamage: Financial losses, regulatory fines, reputational damage

Category: Operational

RiskType: Current

BusinessImpact: Loss of customer trust, regulatory scrutiny, financial penalties

RiskDescription: The risk of not detecting suspicious activities can lead to severe financial and reputati

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement regular system audits", "2": "Enhance employee training on transactio

CreatedAt: 2025-11-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 527:

RiskId: 2192

ComplianceId: 2854

RiskTitle: Delayed Investigation of Suspicious Transactions

Criticality: Medium

PossibleDamage: Financial losses, regulatory fines, reputational damage

Category: Operational
RiskType: Current
BusinessImpact: Increased exposure to financial crimes, regulatory scrutiny
RiskDescription: Failure to promptly investigate flagged transactions can lead to financial losses and re
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear review procedures", "2": "Assign dedicated resources for daily revi
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 528:
RiskId: 2193
ComplianceId: 2855
RiskTitle: Unresolved Audit Findings
Criticality: High
PossibleDamage: Potential regulatory sanctions or financial losses
Category: Operational
RiskType: Current
BusinessImpact: Delayed response to audit findings affecting operational efficiency and compliance sta
RiskDescription: Failure to address audit findings in a timely manner may lead to regulatory non-compl
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear accountability for action plan implementation", "2": "Regular monit
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 529:
RiskId: 2194
ComplianceId: 2856
RiskTitle: Incomplete Action Plan Implementation
Criticality: High
PossibleDamage: Continued non-compliance, repeat audit observations, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Ongoing compliance issues affecting operational efficiency and reputation
RiskDescription: Failure to implement the action plan within agreed timelines may lead to regulatory sc
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 65.7
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear timelines and milestones for action plan implementation", "2": "Reg
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 530:
RiskId: 2195
ComplianceId: 2857
RiskTitle: Financial Losses due to High-Risk Customer Transactions
Criticality: High
PossibleDamage: Financial losses, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Significant financial impact on the institution
RiskDescription: High-risk customers engaging in illicit activities may lead to financial losses and regula

RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence procedures for high-risk customers", "2": "Regular monito
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 531:
RiskId: 2196
ComplianceId: 2858
RiskTitle: Undetected Suspicious Activities
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal actions
Category: Operational
RiskType: Inherent
BusinessImpact: Impact on compliance status, reputation, and financial stability
RiskDescription: Failure to monitor high-risk customers may result in undetected suspicious activities, l
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for transaction monitoring team on identifying suspicious activitie
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 532:
RiskId: 2197

ComplianceId: 2859
RiskTitle: Delayed Reporting of Suspicious Activities
Criticality: High
PossibleDamage: Financial losses, regulatory penalties, reputational harm
Category: Operational
RiskType: Inherent
BusinessImpact: Financial and reputational damage, regulatory scrutiny
RiskDescription: Delay in reporting suspicious activities may lead to severe consequences such as fina
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting procedures and escalation paths", "2": "Regular training
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 533:
RiskId: 2198
ComplianceId: 2860
RiskTitle: Undetected ML/TF Risks
Criticality: High
PossibleDamage: Financial losses and regulatory sanctions
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines and reputational damage
RiskDescription: Failure to identify ML/TF risks may lead to non-compliance with regulations and sever
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Utilize established risk assessment frameworks and tools", "2": "Ensure timely da
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 534:
RiskId: 2199
ComplianceId: 2861
RiskTitle: Misalignment of Risk Appetite with Strategic Objectives
Criticality: High
PossibleDamage: Increased exposure to risks and potential failure to achieve strategic objectives
Category: Operational
RiskType: Residual
BusinessImpact: All business units could be affected by misaligned risk appetite
RiskDescription: Failure to review and update the risk appetite statement could result in misalignment
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear schedule for annual reviews", "2": "Assign responsibility to a dec
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 535:
RiskId: 2200
ComplianceId: 2862
RiskTitle: Lack of Stakeholder Engagement in Risk Appetite Statement Development
Criticality: Medium
PossibleDamage: Risk appetite statement may not accurately reflect the organization's risk tolerance

Category: Operational
RiskType: Residual
BusinessImpact: All business units could be affected by misaligned risk appetite
RiskDescription: Failure to engage stakeholders in the development of the risk appetite statement may
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Conduct regular stakeholder meetings to gather input", "2": "Provide training on ri
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 536:
RiskId: 2201
ComplianceId: 2863
RiskTitle: Inaccurate Client Net Worth Assessment
Criticality: High
PossibleDamage: Incorrect risk assessment and financial exposure calculations
Category: Operational
RiskType: Inherent
BusinessImpact: Client financial stability and investment decisions
RiskDescription: Failure to accurately assess client net worth may result in incorrect risk exposure calc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify collected data through multiple sources", "2": "Implement data validation ch
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 537:
RiskId: 2202
ComplianceId: 2864
RiskTitle: Unauthorized Access to Client Net Worth Data
Criticality: Medium
PossibleDamage: Financial fraud or identity theft
Category: IT
RiskType: Inherent
BusinessImpact: Client data privacy and financial security
RiskDescription: Unauthorized access to client net worth data may result in financial fraud or identity th
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement encryption for data transmission and storage", "2": "Restrict access to
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 538:
RiskId: 2203
ComplianceId: 2865
RiskTitle: Inadequate Source of Wealth Documentation
Criticality: High
PossibleDamage: Increased exposure to money laundering and fraud risks
Category: Compliance
RiskType: Current
BusinessImpact: Potential regulatory fines, loss of reputation, legal actions
RiskDescription: Failure to accurately document clients' sources of wealth may lead to regulatory non-

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence procedures for high-risk clients", "2": "Implement transacti
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 539:
RiskId: 2204
ComplianceId: 2866
RiskTitle: Failure to Verify Source of Wealth
Criticality: High
PossibleDamage: Potential money laundering activities going undetected
Category: Compliance
RiskType: Current
BusinessImpact: Regulatory fines, reputational damage, legal consequences
RiskDescription: Failure to accurately verify the source of wealth may result in the facilitation of money
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated document verification tools", "2": "Conduct periodic audits c
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 540:
RiskId: 2205

ComplianceId: 2867
RiskTitle: Failure to Verify Source of Funds
Criticality: High
PossibleDamage: Potential money laundering or fraud risks
Category: Operational
RiskType: Current
BusinessImpact: Loss of reputation, regulatory fines
RiskDescription: Failure to verify the source of funds may expose the organization to financial and repu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced due diligence for high-risk clients", "2": "Regular document reviews", "3
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 541:
RiskId: 2206
ComplianceId: 2868
RiskTitle: Failure to Verify Source of Wealth
Criticality: High
PossibleDamage: Potential financial crime risks
Category: Operational
RiskType: Current
BusinessImpact: Regulatory fines, legal actions
RiskDescription: Failure to verify the source of wealth information may expose the organization to finan
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Third-party verification services", "2": "Regular audits of verification processes", "3
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 542:
RiskId: 2207
ComplianceId: 2869
RiskTitle: Failure to Detect Suspicious PEP Transactions
Criticality: High
PossibleDamage: Increased risk of money laundering or illicit activities going undetected
Category: Operational
RiskType: Current
BusinessImpact: Financial penalties, reputational damage, regulatory sanctions
RiskDescription: Failure to detect suspicious PEP transactions could result in severe financial and repu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance transaction monitoring algorithms regularly", "2": "Provide ongoing traini
CreatedAt: 2025-11-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 543:
RiskId: 2041
ComplianceId: 2701
RiskTitle: Undetected Internal Control Deficiencies
Criticality: High
PossibleDamage: Financial misstatements, regulatory fines, reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and damage to organizational reputation
RiskDescription: Failure to detect internal control deficiencies may lead to inaccurate financial reportin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a standardized internal control assessment process", "2": "Provide trai
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 544:
RiskId: 2042
ComplianceId: 2702
RiskTitle: Failure to Conduct Audit Committee Reviews
Criticality: High
PossibleDamage: Unidentified risks impacting the organization
Category: Operational
RiskType: Current
BusinessImpact: Financial losses or reputational damage
RiskDescription: Lack of oversight and review by the Audit Committee may result in significant risks go
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular Audit Committee meetings for reviews", "2": "Training for Audit Committe
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 545:
RiskId: 2043
ComplianceId: 2703
RiskTitle: Misstatement of Financial Statements
Criticality: High
PossibleDamage: Financial loss, regulatory fines, reputational damage
Category: Financial
RiskType: Current
BusinessImpact: Finance Department
RiskDescription: Incorrect financial reporting leading to inaccurate decision-making and potential legal
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training on accounting standards", "2": "Engage external audito
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 546:
RiskId: 2044
ComplianceId: 2704
RiskTitle: Lack of External Auditor Oversight
Criticality: Medium
PossibleDamage: Inaccurate financial reporting, lack of independent verification
Category: Financial
RiskType: Current
BusinessImpact: Finance Department
RiskDescription: Failure to obtain independent assessment of financial reporting process leading to po

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular communication with external auditors", "2": "Implement recommendations
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 547:
RiskId: 2045
ComplianceId: 2705
RiskTitle: Undetected Conflict of Interest
Criticality: High
PossibleDamage: Biased decision-making, reputational damage, regulatory fines
Category: Compliance
RiskType: Current
BusinessImpact: Impaired decision-making process and potential legal consequences
RiskDescription: Failure to identify conflicts of interest may result in biased decision-making, reputation
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust conflict of interest disclosure process", "2": "Provide ongoing tra
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 548:
RiskId: 2046

ComplianceId: 2708
RiskTitle: Failure to Meet Audit Committee Meeting Frequency
Criticality: High
PossibleDamage: Delayed decision-making, inadequate oversight
Category: Operational
RiskType: Residual
BusinessImpact: Impact on critical decision-making processes
RiskDescription: Missing meetings may lead to uninformed decisions and lack of oversight on importar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely scheduling of meetings", "2": "Implement backup meeting plans", "3
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 549:
RiskId: 2047
ComplianceId: 2709
RiskTitle: Failure to Notify Audit Committee Members
Criticality: Medium
PossibleDamage: Low attendance, delayed decision-making
Category: Operational
RiskType: Residual
BusinessImpact: Impact on meeting attendance and decision-making process
RiskDescription: Lack of notification may lead to members missing meetings and delays in decision-ma
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Set up automated reminders for notifications", "2": "Establish communication prot

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 550:

RiskId: 2048

ComplianceId: 2710

RiskTitle: Late Agenda Distribution

Criticality: High

PossibleDamage: Inefficient use of meeting time, important topics not adequately addressed

Category: Operational

RiskType: Current

BusinessImpact: Delays in decision-making, potential oversight of critical issues

RiskDescription: Failure to distribute the agenda in a timely manner may result in members not being a

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear deadlines for agenda submission and review", "2": "Implement aut

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 551:

RiskId: 2049

ComplianceId: 2711

RiskTitle: Late Submission of Additional Agenda Items

Criticality: Medium

PossibleDamage: Key topics not adequately addressed, lack of preparation for discussion

Category: Operational
RiskType: Current
BusinessImpact: Inadequate coverage of important issues, potential lack of decision-making readiness
RiskDescription: Late submission of additional agenda items may result in key topics not being adequa
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear deadline for item submission", "2": "Provide guidance on what con
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 552:
RiskId: 2050
ComplianceId: 2712
RiskTitle: Undisclosed Conflicts of Interest
Criticality: High
PossibleDamage: Biased decision-making affecting company integrity
Category: Compliance
RiskType: Current
BusinessImpact: Impaired decision-making, loss of stakeholder trust
RiskDescription: Audit Committee members with undisclosed conflicts of interest may make decisions
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear disclosure requirements", "2": "Regularly review independence crit
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 553:
RiskId: 2051
ComplianceId: 2713
RiskTitle: Non-compliance with Annual Review of Audit Committee Composition
Criticality: High
PossibleDamage: Failure to comply with regulatory requirements, potential conflicts of interest within th
Category: Compliance
RiskType: Current
BusinessImpact: Nomination Committee (NC) and Audit Committee
RiskDescription: Failure to conduct the annual review may lead to regulatory violations and compromis
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication and documentation of the review process", "2": "Prov
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 554:
RiskId: 2052
ComplianceId: 2714
RiskTitle: Undisclosed Conflicts of Interest
Criticality: High
PossibleDamage: Financial misstatements, reputational damage, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Biased decision-making, compromised independence, regulatory non-compliance
RiskDescription: Audit Committee members with undisclosed conflicts of interest may make decisions

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust independence assessment procedures", "2": "Provide ongoing t
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 555:
RiskId: 2053
ComplianceId: 2715
RiskTitle: Undisclosed Financial Relationships
Criticality: High
PossibleDamage: Biased decision-making and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential compromise of audit committee integrity
RiskDescription: Failure to disclose financial relationships may lead to biased decision-making and cor
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on conflict of interest policies", "2": "Establish clear guidelines for
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 556:
RiskId: 2054

ComplianceId: 2716
RiskTitle: Lack of Documented Conflict Mitigation Actions
Criticality: Medium
PossibleDamage: Challenges in proving compliance and effectiveness of conflict mitigation measures
Category: Compliance
RiskType: Inherent
BusinessImpact: Risk of non-compliance and lack of accountability
RiskDescription: Failure to document conflict mitigation actions may result in challenges in proving com
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish standardized documentation procedures", "2": "Regularly review and up
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 557:
RiskId: 2055
ComplianceId: 2717
RiskTitle: Inadequate Training Knowledge
Criticality: High
PossibleDamage: Inadequate knowledge may lead to poor decision-making and non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Audit Committee decisions may be flawed or non-compliant
RiskDescription: Members lacking updated knowledge may not be able to effectively fulfill their roles ar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Provide comprehensive training materials and resources", "2": "Encourage peer-t
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 558:
RiskId: 2056
ComplianceId: 2718
RiskTitle: Appointment of Unqualified Audit Committee Members
Criticality: High
PossibleDamage: Ineffective oversight, potential compliance breaches
Category: Compliance
RiskType: Inherent
BusinessImpact: Impact on audit quality, regulatory compliance, and stakeholder trust
RiskDescription: Appointing unqualified individuals to the Audit Committee may result in inadequate ov
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear qualification criteria for Audit Committee members", "2": "Provide t
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 559:
RiskId: 2057
ComplianceId: 2719
RiskTitle: Mismanagement due to Lack of Clarity in Authority
Criticality: High
PossibleDamage: Ineffective oversight and potential non-compliance

Category: Compliance
RiskType: Inherent
BusinessImpact: Audit Committee operations and regulatory compliance
RiskDescription: Misinterpretation or lack of clarity in the AC's authority may lead to mismanagement, i
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and approval by the Board", "2": "Annual communication to all AC
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 560:
RiskId: 2058
ComplianceId: 2720
RiskTitle: Undisclosed Conflicts of Interest
Criticality: High
PossibleDamage: Biased decision-making, reputational damage, regulatory fines
Category: Compliance
RiskType: Inherent
BusinessImpact: Compromised decision-making, regulatory non-compliance, reputational harm
RiskDescription: Audit Committee members with undisclosed conflicts of interest may make decisions
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear disclosure requirements for potential conflicts of interest", "2": "Pro
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 561:
RiskId: 2059
ComplianceId: 2721
RiskTitle: Non-Compliance with Annual Review of Member Rotation Plan
Criticality: High
PossibleDamage: Non-compliance with tenure limits, lack of knowledge transfer, potential conflicts wit
Category: Operational
RiskType: Current
BusinessImpact: Audit Committee operations and decision-making
RiskDescription: Failure to review and update the member rotation plan annually may lead to non-com
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear timeline for the annual review process", "2": "Provide training to
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 562:
RiskId: 2060
ComplianceId: 2722
RiskTitle: Lack of Experienced Member during Transitions
Criticality: Medium
PossibleDamage: Disruptions in committee operations, lack of knowledge continuity, potential conflicts
Category: Operational
RiskType: Current
BusinessImpact: Audit Committee operations and decision-making
RiskDescription: Failure to retain experienced members during transitions may lead to disruptions in co

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Identify key experienced members for retention in the rotation plan", "2": "Provide
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 563:
RiskId: 2061
ComplianceId: 2723
RiskTitle: Lack of Documentation Risk
Criticality: High
PossibleDamage: Confusion and disputes over delegated authority
Category: Operational
RiskType: Current
BusinessImpact: May lead to delays in decision-making and potential conflicts
RiskDescription: Failure to document delegation of authority may result in misunderstandings and chal
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation requirements", "2": "Internal audits to verify co
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 564:
RiskId: 2062

ComplianceId: 2724
RiskTitle: Non-Disclosure Risk
Criticality: Medium
PossibleDamage: Non-compliance with regulatory requirements
Category: Legal
RiskType: Current
BusinessImpact: May lead to regulatory fines or penalties
RiskDescription: Failure to disclose delegation of authority in the annual report may result in legal cons
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a clear process for reporting delegation in the annual report", "2": "Regu
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 565:
RiskId: 2063
ComplianceId: 2725
RiskTitle: Delay in Decision-making
Criticality: High
PossibleDamage: Inadequate oversight and missed opportunities
Category: Operational
RiskType: Current
BusinessImpact: Impact on critical decision-making processes
RiskDescription: Failure to hold quarterly meetings may lead to delayed decision-making and inadequa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Schedule additional meetings as necessary", "2": "Ensure timely distribution of me

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 566:

RiskId: 2064

ComplianceId: 2726

RiskTitle: Ineffective Agenda Prioritization

Criticality: Medium

PossibleDamage: Critical issues not adequately addressed

Category: Operational

RiskType: Current

BusinessImpact: Impact on decision-making and oversight

RiskDescription: Failure to prioritize agenda items effectively may lead to critical issues not being addr

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear criteria for agenda prioritization", "2": "Seek input from committee m

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 567:

RiskId: 2065

ComplianceId: 2727

RiskTitle: Failure to Schedule Annual Meeting with Auditors

Criticality: High

PossibleDamage: Lack of oversight and communication with auditors leading to potential audit issues

Category: Operational
RiskType: Current
BusinessImpact: Audit oversight and compliance functions compromised
RiskDescription: Failure to schedule the annual meeting with auditors may result in delayed or inadequ
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication channels with auditors throughout the year", "2": "Im
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 568:
RiskId: 2066
ComplianceId: 2728
RiskTitle: Misrepresentation of Decisions
Criticality: High
PossibleDamage: Legal challenges, lack of transparency, erosion of trust in decision-making processe
Category: Compliance
RiskType: Residual
BusinessImpact: May result in incorrect decisions being made or challenges to the validity of decisions
RiskDescription: Failure to document dissenting views may lead to misrepresentation of decisions and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review meeting minutes for completeness and accuracy", "2": "Provide
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 569:
RiskId: 2067
ComplianceId: 2729
RiskTitle: Non-Compliance with Regulatory Requirements
Criticality: High
PossibleDamage: Regulatory fines, penalties, legal actions
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial losses, reputational damage
RiskDescription: Failure to consult with regulators may result in non-compliance with regulatory require
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Promptly escalate unresolved issues to regulators", "2": "Engage legal counsel fo
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 570:
RiskId: 2068
ComplianceId: 2730
RiskTitle: Delayed Submission of Evaluation Forms
Criticality: High
PossibleDamage: Impact on performance review accuracy and decision-making processes
Category: Operational
RiskType: Residual
BusinessImpact: AC performance evaluation process and decision-making effectiveness
RiskDescription: Incomplete or delayed evaluations may result in biased performance reviews and inef

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Set clear deadlines and reminders for form submission", "2": "Provide training on
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 571:
RiskId: 2069
ComplianceId: 2731
RiskTitle: Lack of Discussion on Evaluation Results
Criticality: Medium
PossibleDamage: Stagnant performance and hindered team collaboration
Category: Operational
RiskType: Residual
BusinessImpact: AC team collaboration and performance improvement
RiskDescription: Failure to discuss evaluation results may lead to stagnant performance and hindered
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Allocate sufficient time for discussion in AC meetings", "2": "Encourage open and
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 572:
RiskId: 2070

ComplianceId: 2732
RiskTitle: Engagement of Unqualified Consultant
Criticality: High
PossibleDamage: Inaccurate assessment leading to potential governance issues
Category: Operational
RiskType: Current
BusinessImpact: Audit Committee effectiveness compromised
RiskDescription: Hiring an unqualified consultant may result in a biased or inaccurate assessment of th
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify consultant qualifications and experience", "2": "Define clear assessment sc
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 573:
RiskId: 2071
ComplianceId: 2733
RiskTitle: Ineffective Committee Performance
Criticality: High
PossibleDamage: Failure to make informed decisions and achieve committee objectives
Category: Operational
RiskType: Inherent
BusinessImpact: Delays in decision-making, potential errors in judgment
RiskDescription: AC members may lack necessary skills to contribute effectively to committee discussi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Provide targeted training programs for identified skill gaps", "2": "Encourage ment

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 574:

RiskId: 2072

ComplianceId: 2734

RiskTitle: Outdated Skills and Knowledge Among AC Members

Criticality: High

PossibleDamage: Ineffective decision-making and potential compliance violations

Category: Operational

RiskType: Inherent

BusinessImpact: Impact on all business units relying on AC decisions

RiskDescription: AC members lacking necessary skills and knowledge may make decisions that are nc

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update the list of recommended training programs based on industry tre

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 575:

RiskId: 2073

ComplianceId: 2735

RiskTitle: Conflicts of Interest Due to Undisclosed Shareholdings

Criticality: High

PossibleDamage: Legal penalties, loss of reputation, and financial harm

Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal investigations, fines, and loss of stakeholder trust
RiskDescription: Failure to disclose significant shareholdings may result in conflicts of interest, insider t
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust disclosure processes", "2": "Conduct regular audits of disclosed
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 576:
RiskId: 2074
ComplianceId: 2736
RiskTitle: Non-compliance with IPT approval process
Criticality: High
PossibleDamage: Legal penalties, loss of shareholder trust
Category: Compliance
RiskType: Residual
BusinessImpact: Audit Committee credibility and company reputation
RiskDescription: Failure to comply with IPT approval process may result in legal consequences and da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear criteria for evaluation", "2": "Provide training to Audit Committee m
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 577:
RiskId: 2075
ComplianceId: 2737
RiskTitle: Failure to Identify IPTs
Criticality: High
PossibleDamage: Conflicts of interest, reputational damage, regulatory penalties
Category: Compliance
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to identify IPTs could result in non-compliance with regulatory requirements, c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training sessions for staff on identifying IPTs", "2": "Engage ext
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 578:
RiskId: 2076
ComplianceId: 2738
RiskTitle: Failure to Disclose RPTs
Criticality: High
PossibleDamage: Financial misstatements, legal issues, investor distrust
Category: Compliance
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to disclose RPTs accurately could result in financial misstatements, legal repe

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a robust RPT disclosure process with clear approval levels", "2": "Condu
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 579:
RiskId: 2077
ComplianceId: 2739
RiskTitle: Undisclosed Related Party Transactions
Criticality: High
PossibleDamage: Financial loss, reputational damage, regulatory fines
Category: Compliance
RiskType: Residual
BusinessImpact: Audit Committee credibility, regulatory compliance
RiskDescription: Failure to disclose related party transactions can lead to conflicts of interest, financial
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict disclosure policies for related party transactions", "2": "Regular m
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 580:
RiskId: 2078

ComplianceId: 2740
RiskTitle: Misreported Transactions
Criticality: Medium
PossibleDamage: Legal disputes, reputational damage, financial loss
Category: Compliance
RiskType: Residual
BusinessImpact: Loss of trust, legal liabilities
RiskDescription: Inaccurate or misleading reporting of transactions with associates can lead to legal di
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated reporting systems for transactions", "2": "Regular audits of
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 581:
RiskId: 2079
ComplianceId: 2741
RiskTitle: Inaccurate Reporting of IPTs
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: May lead to incorrect decision-making and financial losses
RiskDescription: Failure to accurately report IPTs may result in incorrect decisions by the AC, leading t
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement regular training for management on reporting requirements", "2": "Con

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 582:

RiskId: 2080

ComplianceId: 2742

RiskTitle: Biased Selection of IFAs

Criticality: High

PossibleDamage: Incorrect advice leading to financial losses on significant IPTs

Category: Operational

RiskType: Inherent

BusinessImpact: Finance Department

RiskDescription: The risk of selecting biased IFAs who may provide incorrect advice on significant IPTs

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement a thorough vetting process for IFAs", "2": "Regularly monitor the perfor

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 583:

RiskId: 2081

ComplianceId: 2743

RiskTitle: Undisclosed Conflicts of Interest

Criticality: High

PossibleDamage: Biased decision-making, legal consequences

Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal actions, loss of trust
RiskDescription: Failure to disclose interests may lead to biased decision-making or legal actions agair
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reminders for submission deadlines", "2": "Conduct regular
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 584:
RiskId: 2082
ComplianceId: 2744
RiskTitle: Failure to Review Transactions with Related Parties
Criticality: High
PossibleDamage: Reputational harm, legal consequences, financial losses
Category: Compliance
RiskType: Current
BusinessImpact: Potential conflicts of interest, regulatory fines, shareholder lawsuits
RiskDescription: Failure to review transactions with related parties could result in non-compliance with
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust review process with clear criteria", "2": "Seek independent leg
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 585:
RiskId: 2083
ComplianceId: 2745
RiskTitle: Non-Disclosure of RPTs
Criticality: High
PossibleDamage: Legal consequences, reputational damage, loss of shareholder trust
Category: Compliance
RiskType: Residual
BusinessImpact: Finance Department
RiskDescription: Failure to disclose RPTs can lead to regulatory penalties, legal actions, and negative
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust internal controls for identifying and disclosing RPTs", "2": "Regu
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 586:
RiskId: 2084
ComplianceId: 2746
RiskTitle: Non-Disclosure of IPTs
Criticality: High
PossibleDamage: Regulatory fines, legal risks, loss of shareholder trust
Category: Compliance
RiskType: Residual
BusinessImpact: Finance Department
RiskDescription: Failure to disclose IPTs can lead to regulatory sanctions, legal liabilities, and erosion

RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear policies and procedures for identifying and disclosing IPTs", "2": "F
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 587:
RiskId: 2085
ComplianceId: 2747
RiskTitle: Underreporting of Concerns
Criticality: High
PossibleDamage: Legal investigations, reputational damage, financial penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to establish multiple reporting channels may lead to underreporting of concern
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly communicate and educate employees on reporting channels", "2": "Cor
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 588:
RiskId: 2086

ComplianceId: 2748
RiskTitle: Breach of Confidentiality
Criticality: High
PossibleDamage: Retaliation against whistle-blowers, loss of trust in reporting mechanisms
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to utilize secure systems for reporting may lead to breaches of confidentiality,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption and access controls for reporting systems", "2": "Regularly
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 589:
RiskId: 2087
ComplianceId: 2749
RiskTitle: Delayed Investigation of Whistle-blowing Reports
Criticality: High
PossibleDamage: Legal actions, unresolved issues, damaged reputation
Category: Operational
RiskType: Current
BusinessImpact: Delayed investigations can lead to legal liabilities, unresolved issues affecting operati
RiskDescription: Failure to investigate whistle-blowing reports promptly may result in legal consequenc
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear escalation procedures for delayed investigations", "2": "Provide re

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 590:

RiskId: 2088

ComplianceId: 2750

RiskTitle: Risk of Whistle-Blower Retaliation

Criticality: High

PossibleDamage: Risk of harm or retaliation against whistle-blowers

Category: Operational

RiskType: Residual

BusinessImpact: Potential harm to whistle-blowers and loss of trust in reporting mechanisms.

RiskDescription: Failure to maintain whistle-blower confidentiality could lead to serious consequences

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strict access controls", "2": "Regularly train employees on confidentiali

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 591:

RiskId: 2089

ComplianceId: 2751

RiskTitle: Risk of Whistle-Blower Silence

Criticality: Medium

PossibleDamage: Risk of crucial information not being reported

Category: Operational
RiskType: Residual
BusinessImpact: Potential risks not being addressed and organizational vulnerabilities remaining unad
RiskDescription: If whistle-blowers do not feel safe to report, the organization may miss critical informa
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish anonymous reporting channels", "2": "Provide legal protection for whistl
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 592:
RiskId: 2090
ComplianceId: 2752
RiskTitle: Lack of Awareness on Whistle-blowing Policy
Criticality: High
PossibleDamage: Underreporting of misconduct and potential legal implications
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Employees may fail to report misconduct due to lack of awareness, leading to potentia
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on the policy", "2": "Clear communication on reporting c
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 593:
RiskId: 2091
ComplianceId: 2753
RiskTitle: Lack of New Employee Onboarding Training on Whistle-blowing Policy
Criticality: Medium
PossibleDamage: Missed reporting opportunities and potential misconduct going unreported
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: New employees may not report misconduct due to lack of awareness, leading to pote
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Incorporate policy training into onboarding process", "2": "Provide ongoing suppor
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 594:
RiskId: 2092
ComplianceId: 2754
RiskTitle: Failure to Conduct Annual Review by Audit Committee
Criticality: High
PossibleDamage: Ineffective whistle-blowing policy and legal non-compliance
Category: Compliance
RiskType: Current
BusinessImpact: All business units may face legal consequences and reputational damage.
RiskDescription: Failure to conduct the annual review may lead to an outdated or ineffective whistle-blo

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly communicate the importance of the review process", "2": "Provide traini
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 595:
RiskId: 2093
ComplianceId: 2755
RiskTitle: Appointment of Unqualified Legal Counsel
Criticality: High
PossibleDamage: Incomplete or biased investigations, legal challenges, reputational damage
Category: Legal
RiskType: Inherent
BusinessImpact: Legal and reputational risks
RiskDescription: Appointing legal counsel without fraud investigation expertise may result in compromi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Thorough vetting of legal counsel candidates", "2": "Establish clear conflict of inte
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 596:
RiskId: 2094

ComplianceId: 2756
RiskTitle: Delay in Appointing Investigators
Criticality: Medium
PossibleDamage: Evidence tampering, witness intimidation, loss of critical information
Category: Operational
RiskType: Inherent
BusinessImpact: Operational and legal risks
RiskDescription: Delay in appointing investigators may result in compromised investigations, loss of cri
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear escalation procedures for whistle-blowing reports", "2": "Implemen
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 597:
RiskId: 2095
ComplianceId: 2757
RiskTitle: Delay in Reporting Investigation Findings
Criticality: High
PossibleDamage: Missed opportunities for corrective actions and impact on organizational reputation
Category: Operational
RiskType: Current
BusinessImpact: Compromised decision-making processes
RiskDescription: Failure to report investigation findings in a timely manner may result in missed opportu
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear reporting timelines and escalation procedures", "2": "Regular moni

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 598:

RiskId: 2096

ComplianceId: 2758

RiskTitle: Breach of Whistle-blower Confidentiality

Criticality: Medium

PossibleDamage: Unauthorized access to sensitive information leading to breach of whistle-blower co

Category: Operational

RiskType: Current

BusinessImpact: Compromise of whistle-blower confidentiality and trust in the reporting process

RiskDescription: Failure to secure communication channels may result in unauthorized access to sens

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement encryption and secure communication channels", "2": "Restrict access

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 599:

RiskId: 2097

ComplianceId: 2759

RiskTitle: Failure to Conduct Annual Independence Assessment

Criticality: High

PossibleDamage: Conflicts of interest, compromised audit quality, regulatory fines, reputational damag

Category: Compliance
RiskType: Current
BusinessImpact: Audit quality, regulatory compliance, stakeholder trust
RiskDescription: Not conducting the annual independence assessment could lead to conflicts of interes
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a rotation policy for audit firms to reduce familiarity threat", "2": "Engag
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 600:
RiskId: 2098
ComplianceId: 2760
RiskTitle: Non-compliance with Auditor Fee Disclosure Requirements
Criticality: High
PossibleDamage: Potential damage includes regulatory fines, reputational damage, and loss of investo
Category: Compliance
RiskType: Current
BusinessImpact: All business units would be impacted by potential regulatory fines and reputational da
RiskDescription: Failure to disclose accurate auditor fees could result in regulatory non-compliance, leg
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust financial controls and oversight mechanisms", "2": "Conduct reg
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 601:
RiskId: 2099
ComplianceId: 2761
RiskTitle: Delayed Access to Information
Criticality: High
PossibleDamage: Delays in decision-making and investigations
Category: Operational
RiskType: Inherent
BusinessImpact: Impacts the efficiency and effectiveness of the Audit Committee
RiskDescription: Failure to promptly provide access to information requested by the Audit Committee C
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear timelines for responding to access requests", "2": "Implement auto
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 602:
RiskId: 2100
ComplianceId: 2762
RiskTitle: Delayed Access Approval
Criticality: Medium
PossibleDamage: Lack of access to relevant data impacting decision-making
Category: Operational
RiskType: Inherent
BusinessImpact: May hinder the Audit Committee's ability to fulfill its responsibilities effectively
RiskDescription: Failure to promptly grant access to information requested by the Audit Committee Cha

RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated access approval workflows", "2": "Establish escalation proc
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 603:
RiskId: 2101
ComplianceId: 2763
RiskTitle: Missed Meeting Notices
Criticality: High
PossibleDamage: Members missing important meetings, decisions being delayed
Category: Operational
RiskType: Residual
BusinessImpact: Audit Committee operations and decision-making process
RiskDescription: Failure to distribute meeting notices may result in members not being able to attend o
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Send reminders to members a few days before the meeting", "2": "Implement an a
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 604:
RiskId: 2102

ComplianceId: 2764
RiskTitle: Delayed Meeting Minutes Circulation
Criticality: Medium
PossibleDamage: Misinterpretation of decisions, lack of accountability, disputes among committee mer
Category: Operational
RiskType: Residual
BusinessImpact: Audit Committee operations and decision-making process
RiskDescription: Delay in circulating meeting minutes may lead to misinterpretation of decisions, lack c
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a standardized template for meeting minutes to streamline the documer
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 605:
RiskId: 2103
ComplianceId: 2765
RiskTitle: Subjective Performance Evaluations
Criticality: High
PossibleDamage: Inaccurate assessment of committee performance and potential conflicts within the c
Category: Operational
RiskType: Inherent
BusinessImpact: May lead to ineffective decision-making and lack of accountability within the committe
RiskDescription: Subjective evaluations may result in biased assessments and hinder the committee's
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement clear and objective performance criteria", "2": "Regularly monitor and r

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 606:

RiskId: 2104

ComplianceId: 2766

RiskTitle: Lack of Documentation and Oversight

Criticality: Medium

PossibleDamage: Decreased transparency and accountability in committee evaluations.

Category: Operational

RiskType: Inherent

BusinessImpact: May lead to challenges in identifying performance issues and addressing conflicts wit

RiskDescription: Failure to document and present evaluation results may hinder the Board's ability to o

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear documentation guidelines", "2": "Regular reporting to the Board or

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 607:

RiskId: 2105

ComplianceId: 2767

RiskTitle: Non-Disclosure of Evaluation Results

Criticality: High

PossibleDamage: Decreased trust from stakeholders, regulatory fines, reputational damage

Category: Compliance
RiskType: Residual
BusinessImpact: Audit Committee effectiveness, stakeholder relationships, company reputation
RiskDescription: Failure to disclose evaluation results in the Annual Report may result in stakeholders
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of evaluation completion deadlines", "2": "Establish clear com
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 608:
RiskId: 2106
ComplianceId: 2768
RiskTitle: Non-Compliance with Announcement Requirements
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal actions
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential loss of investor trust and legal consequences
RiskDescription: Failure to announce loan provisions to joint ventures may result in allegations of unfai
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for Audit Committee members on compliance requirements", "2":
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 609:
RiskId: 2107
ComplianceId: 2769
RiskTitle: Lack of Clarity in Transaction Terms
Criticality: High
PossibleDamage: Legal challenges and loss of shareholder trust
Category: Compliance
RiskType: Current
BusinessImpact: Audit Committee credibility and shareholder confidence
RiskDescription: Failure to provide a clear opinion on transaction terms may lead to misunderstandings
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Thoroughly review transaction terms", "2": "Seek legal advice if uncertain", "3": "C
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 610:
RiskId: 2108
ComplianceId: 2770
RiskTitle: Late Distribution of Circular
Criticality: Medium
PossibleDamage: Legal challenges and shareholder dissatisfaction
Category: Compliance
RiskType: Current
BusinessImpact: Shareholder perception and compliance reputation
RiskDescription: Delaying the distribution of the circular may lead to misunderstandings and negative p

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear distribution timelines", "2": "Implement reminders and tracking mec
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 611:
RiskId: 2109
ComplianceId: 2771
RiskTitle: Inadequate Reporting Mechanisms
Criticality: High
PossibleDamage: Lack of timely reporting and resolution of concerns
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to establish effective reporting mechanisms may result in delayed or missed re
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of hotline and email for prompt response", "2": "Training empl
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 612:
RiskId: 2110

ComplianceId: 2772
RiskTitle: Delayed Resolution of Reported Concerns
Criticality: Medium
PossibleDamage: Delayed resolution of reported concerns
Category: Operational
RiskType: Inherent
BusinessImpact: Audit Committee and investigative team
RiskDescription: Failure to acknowledge and investigate reports in a timely manner may lead to unresc
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear escalation procedures for unresolved concerns", "2": "Regular mor
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 613:
RiskId: 2111
ComplianceId: 2773
RiskTitle: Ineffective Risk Management Systems Documentation Review
Criticality: High
PossibleDamage: Failure to identify risks and implement effective risk management processes
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, regulatory non-compliance, and reputational damage
RiskDescription: Inadequate review of risk management systems documentation may lead to unidentifi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear communication channels between management and the Audit Co

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 614:

RiskId: 2112

ComplianceId: 2774

RiskTitle: Inaccurate Reporting on Internal Controls

Criticality: High

PossibleDamage: Mismanagement of risks, regulatory non-compliance, reputational damage

Category: Operational

RiskType: Current

BusinessImpact: Impacts decision-making processes and regulatory compliance

RiskDescription: Failure to provide accurate and comprehensive reporting on internal controls may lea

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement regular internal control assessments", "2": "Engage external auditors f

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 615:

RiskId: 2113

ComplianceId: 2775

RiskTitle: Lack of Expertise in Audit Committee

Criticality: High

PossibleDamage: Ineffective oversight of risk management and internal controls

Category: Operational
RiskType: Inherent
BusinessImpact: Inadequate risk management practices and potential control failures
RiskDescription: Audit Committee members lacking necessary skills and qualifications to effectively as
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training programs to address identified gaps", "2": "Engage external advis
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 616:
RiskId: 2114
ComplianceId: 2776
RiskTitle: Lack of Documentation and Sharing of Assessment Results
Criticality: Medium
PossibleDamage: Lack of transparency and accountability in addressing skills gaps
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of oversight and potential misalignment in training needs
RiskDescription: Failure to document and share assessment results may lead to miscommunication an
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear documentation procedures", "2": "Regularly review and update tra
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 617:
RiskId: 2115
ComplianceId: 2777
RiskTitle: Inadequate Oversight Expertise
Criticality: High
PossibleDamage: Inadequate oversight capabilities and potential compliance failures
Category: Operational
RiskType: Current
BusinessImpact: Reduced effectiveness of Audit Committee oversight
RiskDescription: Lack of expertise in critical areas may lead to oversight failures and potential compliar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular training sessions for Audit Committee members to enhance expe
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 618:
RiskId: 2116
ComplianceId: 2778
RiskTitle: Lack of Transparency in External Advisor Engagements
Criticality: Medium
PossibleDamage: Questions regarding transparency and accountability in the oversight process
Category: Operational
RiskType: Current
BusinessImpact: Reduced trust in Audit Committee processes
RiskDescription: Failure to document and report external advisor engagements may raise concerns ab

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a standardized template for documenting external advisor engagements
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 619:
RiskId: 2117
ComplianceId: 2779
RiskTitle: Ineffective Collaboration with Board Risk Committee
Criticality: High
PossibleDamage: Ineffective risk oversight and decision-making
Category: Operational
RiskType: Inherent
BusinessImpact: Compromised risk management processes and potential financial losses
RiskDescription: Lack of coordination and information sharing between Audit Committee and Board Ris
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication channels between committees", "2": "Regularly rev
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 620:
RiskId: 2118

ComplianceId: 2780
RiskTitle: Outdated Risk Management Policies
Criticality: High
PossibleDamage: Ineffective risk mitigation strategies
Category: Operational
RiskType: Inherent
BusinessImpact: Compromised decision-making processes
RiskDescription: Outdated risk management policies may not adequately address current risk exposur
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular annual review of policies", "2": "Engagement of relevant stakeholders", "3
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 621:
RiskId: 2119
ComplianceId: 2781
RiskTitle: Unidentified Risks
Criticality: High
PossibleDamage: Financial losses due to unidentified risks
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may suffer financial losses
RiskDescription: Failure to identify and address risks may lead to financial losses and operational disru
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular risk assessment workshops", "2": "Utilization of risk management softwar
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 622:
RiskId: 2120
ComplianceId: 2782
RiskTitle: Outdated Risk Management Framework
Criticality: Medium
PossibleDamage: Ineffective risk mitigation due to outdated practices
Category: Operational
RiskType: Inherent
BusinessImpact: Audit and Risk Committee may face challenges in effective risk governance
RiskDescription: An outdated risk management framework may lead to ineffective risk mitigation strate
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish quarterly review meetings", "2": "Utilize risk management software for tr
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 623:
RiskId: 2121
ComplianceId: 2783
RiskTitle: Undetected Control Deficiencies
Criticality: High
PossibleDamage: Financial losses and regulatory non-compliance

Category: Operational
RiskType: Residual
BusinessImpact: All business units within the organization may be impacted
RiskDescription: Failure to detect control deficiencies may lead to financial losses and regulatory pena
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust internal control framework", "2": "Regular training and awaren
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 624:
RiskId: 2122
ComplianceId: 2784
RiskTitle: Failure to Provide Quarterly Risk Reports
Criticality: High
PossibleDamage: Inadequate risk management decisions by the Board
Category: Operational
RiskType: Current
BusinessImpact: All business units may suffer from ineffective risk management strategies
RiskDescription: Failure to provide timely and relevant risk reports may lead to uninformed decision-ma
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish automated reminders for timely reporting", "2": "Implement regular traini
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 625:
RiskId: 2123
ComplianceId: 2785
RiskTitle: Inadequate Key Risk Indicators (KRIs) Monitoring
Criticality: High
PossibleDamage: Undetected risks, control weaknesses, regulatory non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: Impact on risk management effectiveness and regulatory compliance
RiskDescription: Failure to monitor KRIs effectively may result in unidentified risks, control weaknesses
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on KRI identification and monitoring procedures", "2": "Implemen
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 626:
RiskId: 2124
ComplianceId: 2786
RiskTitle: Inadequate Quarterly Reporting to Audit Committee
Criticality: High
PossibleDamage: Inadequate oversight of risks, control failures, increased exposure to risks
Category: Operational
RiskType: Current
BusinessImpact: Audit Committee's ability to assess internal controls and risk management processes
RiskDescription: Failure to provide timely and accurate quarterly reports to the Audit Committee may re

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely and accurate reporting", "2": "Implement regular review processes"
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 627:
RiskId: 2125
ComplianceId: 2787
RiskTitle: Misalignment on Risk Tolerance Levels
Criticality: High
PossibleDamage: Unexpected losses, reputation damage, regulatory non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may be impacted
RiskDescription: Failure to define risk tolerance levels annually may result in misalignment on risk acce
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular communication and collaboration between the Audit Committee and the
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 628:
RiskId: 2126

ComplianceId: 2788
RiskTitle: Inadequate Assessment of Internal Control Principles
Criticality: High
PossibleDamage: Undetected risks, financial losses, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Failure to assess internal control principles may result in ineffective risk management
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training programs on internal control principles", "2": "Enhance
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 629:
RiskId: 2127
ComplianceId: 2789
RiskTitle: Ineffective Risk Management Policy
Criticality: High
PossibleDamage: Increased exposure to unidentified risks, financial losses, reputational damage, regu
Category: Operational
RiskType: Inherent
BusinessImpact: All business units would be affected by unmanaged risks
RiskDescription: Failure to develop a comprehensive risk management policy may result in the organiz
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Engage relevant stakeholders in policy development process", "2": "Conduct thor

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 630:

RiskId: 2128

ComplianceId: 2790

RiskTitle: Undetected Risks

Criticality: High

PossibleDamage: Financial losses or operational disruptions

Category: Operational

RiskType: Inherent

BusinessImpact: All business units may be affected by unidentified risks.

RiskDescription: Failure to conduct timely risk assessments may result in undetected risks that could le

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement regular training for risk owners on conducting effective risk assessmen

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 631:

RiskId: 2129

ComplianceId: 2791

RiskTitle: Unidentified Risks and Control Weaknesses

Criticality: High

PossibleDamage: Financial losses, regulatory non-compliance

Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to identify and address significant control weaknesses may result in financial l
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on control self-assessment procedures", "2": "Internal audits to v
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 632:
RiskId: 2130
ComplianceId: 2792
RiskTitle: Failure to Report Significant Deficiencies
Criticality: High
PossibleDamage: Increased risk exposure, potential fraud incidents going unnoticed, and ineffective in
Category: Operational
RiskType: Residual
BusinessImpact: All business units could be impacted by increased operational risks and potential fina
RiskDescription: Failure to report significant deficiencies may result in material misstatements in financ
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training for management on identifying and reporting significan
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 633:
RiskId: 2131
ComplianceId: 2793
RiskTitle: Undetected Fraud Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage for the organization
RiskDescription: Failure to detect and address fraud risks may lead to financial losses, reputational da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular fraud risk training for employees", "2": "Enhance whistleblower
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 634:
RiskId: 2132
ComplianceId: 2794
RiskTitle: Failure to Initiate Fraud Investigation Protocol
Criticality: High
PossibleDamage: Prolonged exposure to fraud risks and potential financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, reputational damage, and regulatory penalties
RiskDescription: Failure to promptly initiate the fraud investigation protocol may result in undetected fra

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Convene the Audit Committee immediately upon suspicion of fraud", "2": "Engage
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 635:
RiskId: 2133
ComplianceId: 2795
RiskTitle: Failure to Report Investigation Findings to Audit Committee
Criticality: Medium
PossibleDamage: Inadequate remediation actions and ongoing fraud risks
Category: Operational
RiskType: Inherent
BusinessImpact: Reputational damage, regulatory penalties, and financial losses
RiskDescription: Not reporting investigation findings to the Audit Committee may result in unresolved fr
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting protocols for auditors", "2": "Regularly update the Audit C
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 636:
RiskId: 2134

ComplianceId: 2796
RiskTitle: Undetected Vulnerabilities and System Weaknesses
Criticality: High
PossibleDamage: Increased risk of financial losses and regulatory non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Internal Audit Team
RiskDescription: Failure to detect critical vulnerabilities and weaknesses in internal controls and risk m
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on data analytics tools", "2": "Continuous monitoring of system pe
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 637:
RiskId: 2135
ComplianceId: 2797
RiskTitle: Unidentified Vulnerabilities and System Failures
Criticality: Medium
PossibleDamage: Increased risk of system failures and data breaches
Category: Operational
RiskType: Current
BusinessImpact: Internal Audit Team
RiskDescription: Failure to identify key vulnerabilities in internal controls and risk management process
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regular review of testing methodologies", "2": "Engagement with external auditors

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 638:

RiskId: 2136

ComplianceId: 2798

RiskTitle: Failure to Conduct Annual Independent Review

Criticality: High

PossibleDamage: Unidentified risks, compliance violations, ineffective internal controls

Category: Operational

RiskType: Residual

BusinessImpact: All business units

RiskDescription: Failure to conduct annual independent reviews may lead to unidentified risks, compli

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Ensure timely engagement of external consultants", "2": "Implement recommenda

CreatedAt: 2025-11-03 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 639:

RiskId: 2137

ComplianceId: 2799

RiskTitle: Ineffective Internal Audit Oversight

Criticality: High

PossibleDamage: Increased risk of non-compliance and potential regulatory penalties

Category: Compliance
RiskType: Inherent
BusinessImpact: Audit Committee and overall organization
RiskDescription: Failure to review and approve the internal audit plan may result in inadequate coverag
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of internal audit activities", "2": "Training for Audit Committee
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 640:
RiskId: 2138
ComplianceId: 2800
RiskTitle: Incomplete Internal Control Assessment
Criticality: Medium
PossibleDamage: Increased risk of control failures and potential compliance breaches
Category: Compliance
RiskType: Inherent
BusinessImpact: Internal Audit Team and overall organization
RiskDescription: Failure to benchmark against the COSO framework may result in incomplete assessm
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Training for internal audit team on COSO framework", "2": "Regular review of ben
CreatedAt: 2025-11-03 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 641:
RiskId: 1863
ComplianceId: 2517
RiskTitle: Undetected Vulnerabilities in Remittance Corridors
Criticality: High
PossibleDamage: Potential money laundering activities due to unidentified vulnerabilities
Category: Operational
RiskType: Inherent
BusinessImpact: Compliance and Risk Management Teams
RiskDescription: Failure to identify vulnerabilities in remittance corridors may lead to exploitation by mo
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Increase frequency of vulnerability assessments", "2": "Enhance monitoring contr
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 642:
RiskId: 1864
ComplianceId: 2518
RiskTitle: Ineffective Implementation of Preventive Measures
Criticality: High
PossibleDamage: Increased vulnerability to risks and potential financial losses
Category: Operational
RiskType: Residual
BusinessImpact: All business units within the remittance corridor may experience financial losses and
RiskDescription: Failure to implement tailored preventive measures may result in an increased likeliho

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting on the implementation progress", "2": "Training
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 643:
RiskId: 1865
ComplianceId: 2519
RiskTitle: Failure to Identify High-Risk Customers
Criticality: High
PossibleDamage: Increased exposure to money laundering and terrorist financing activities, regulatory
Category: Compliance
RiskType: Current
BusinessImpact: Compliance and Risk Analysis Department
RiskDescription: Failure to identify high-risk customers may lead to increased exposure to money laun
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced customer due diligence procedures", "2": "Regular training for analysts
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 644:
RiskId: 1866

ComplianceId: 2520
RiskTitle: Inadequate Customer Survey Analysis
Criticality: Medium
PossibleDamage: Incomplete risk assessment, increased exposure to money laundering and terrorist f
Category: Compliance
RiskType: Current
BusinessImpact: Compliance and Risk Analysis Department
RiskDescription: Inadequate customer survey analysis may result in incomplete risk assessment and i
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular customer survey campaigns", "2": "Integration of survey results into risk a
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 645:
RiskId: 1867
ComplianceId: 2521
RiskTitle: Ineffective Preventive Measures
Criticality: High
PossibleDamage: Increased risk of money laundering and financial crimes
Category: Compliance
RiskType: Residual
BusinessImpact: Compliance Department
RiskDescription: Failure to detect and prevent money laundering activities due to ineffective preventive
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement enhanced monitoring procedures", "2": "Provide additional training to F

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 646:

RiskId: 1868

ComplianceId: 2522

RiskTitle: Inaccurate Compliance Reporting

Criticality: Medium

PossibleDamage: Inaccurate assessment of preventive measures

Category: Compliance

RiskType: Residual

BusinessImpact: Compliance Department

RiskDescription: Misinterpretation of compliance reports may lead to inadequate oversight of preventiv

RiskLikelihood: 5

RiskImpact: 7

RiskExposureRating: 35

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement automated compliance monitoring tools", "2": "Conduct regular training

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 647:

RiskId: 1869

ComplianceId: 2523

RiskTitle: Ineffective Cross-Border Cooperation

Criticality: High

PossibleDamage: Increased risks of financial crimes due to lack of effective collaboration

Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses and damage to reputation
RiskDescription: Failure to effectively assess cooperation agreements may result in insufficient informa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of cooperation agreements", "2": "Enhanced commun
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 648:
RiskId: 1870
ComplianceId: 2524
RiskTitle: Lack of Stakeholder Feedback
Criticality: Medium
PossibleDamage: Missed opportunities for improving cooperation effectiveness
Category: Operational
RiskType: Current
BusinessImpact: Potential inefficiencies in collaboration efforts
RiskDescription: Not conducting stakeholder interviews may lead to a lack of critical feedback on cross
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Structured interview process with predefined questions", "2": "Analysis of stakeho
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 649:
RiskId: 1871
ComplianceId: 2525
RiskTitle: Undetected Risks in AML/CFT Regime
Criticality: High
PossibleDamage: Increased vulnerability to money laundering and terrorist financing activities
Category: Compliance
RiskType: Current
BusinessImpact: Potential regulatory fines and reputational damage
RiskDescription: Failure to analyze corruption impact may lead to undetected risks in the AML/CFT reg
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance internal controls and monitoring mechanisms", "2": "Conduct regular aud
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 650:
RiskId: 1872
ComplianceId: 2526
RiskTitle: Inaccurate ML/TF Consequence Assessment
Criticality: High
PossibleDamage: Misinformed decision-making and increased ML/TF risks
Category: Operational
RiskType: Inherent
BusinessImpact: All business units relying on accurate ML/TF consequence data for risk assessment.
RiskDescription: Failure to collect accurate data may lead to misinformed decisions and ineffective risk

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for FIU staff on data collection procedures", "2": "Implement data
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 651:
RiskId: 1873
ComplianceId: 2527
RiskTitle: Flawed Data Analysis for Consequence Assessment
Criticality: Medium
PossibleDamage: Inaccurate consequence assessments and ineffective risk mitigation strategies
Category: Operational
RiskType: Inherent
BusinessImpact: CRA department's ability to accurately assess ML/TF consequences.
RiskDescription: Relying solely on internal analysis may lead to biased assessments and flawed conse
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a panel of subject matter experts for consultations", "2": "Document exp
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 652:
RiskId: 1874

ComplianceId: 2528
RiskTitle: Inadequate Evaluation of Risk-Mitigating Measures
Criticality: High
PossibleDamage: Inadequate evaluation could lead to ineffective risk mitigation, increased exposure to
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance Department and overall business operations
RiskDescription: Failure to adequately evaluate risk-mitigating measures could result in ineffective risk
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear evaluation criteria and metrics for risk-mitigating measures", "2": "I
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 653:
RiskId: 1875
ComplianceId: 2529
RiskTitle: Increased Money Laundering and Terrorist Financing Risks
Criticality: High
PossibleDamage: Increased exposure to money laundering and terrorist financing activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Risk assessment teams within regulatory bodies and financial institutions
RiskDescription: Failure to conduct an annual risk assessment of informal remittance channels may res
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement enhanced due diligence procedures for high-risk transactions", "2": "Pr

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 654:

RiskId: 1876

ComplianceId: 2530

RiskTitle: Inadequate Understanding of ML/TF Risks in Informal Remittance Channels

Criticality: Medium

PossibleDamage: Inadequate understanding of ML/TF risks in informal remittance channels

Category: Compliance

RiskType: Inherent

BusinessImpact: Regulatory bodies and financial institutions

RiskDescription: Failure to collect data on the volume and nature of informal remittance transactions m

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement robust data collection mechanisms", "2": "Utilize data analytics tools fo

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 655:

RiskId: 1877

ComplianceId: 2531

RiskTitle: Inadequate Risk Mitigation Measures

Criticality: High

PossibleDamage: Increased exposure to financial crimes and regulatory penalties

Category: Compliance
RiskType: Inherent
BusinessImpact: Financial institutions and regulatory bodies overseeing remittance services
RiskDescription: Failure to implement effective risk mitigation measures may lead to regulatory non-co
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on risk mitigation measures", "2": "Con
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 656:
RiskId: 1878
ComplianceId: 2532
RiskTitle: Outdated Risk Mitigation Measures
Criticality: Medium
PossibleDamage: Vulnerabilities in remittance mechanisms due to outdated measures
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial institutions and regulatory bodies overseeing remittance services
RiskDescription: Failure to review and update risk mitigation measures bi-annually may expose the org
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular risk assessment updates to identify new risks", "2": "Engagement with ind
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 657:
RiskId: 1879
ComplianceId: 2533
RiskTitle: Undetected ML/TF Risks in Remittance Corridors
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of license
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal and financial consequences
RiskDescription: Failure to conduct annual ML/TF risk assessments may result in undetected money la
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance monitoring and reporting mechanisms", "2": "Implement enhanced due d
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 658:
RiskId: 1880
ComplianceId: 2534
RiskTitle: Inconsistent ML/TF Risk Assessment Methodologies
Criticality: Medium
PossibleDamage: Inaccurate risk evaluations, ineffective risk mitigation strategies
Category: Operational
RiskType: Inherent
BusinessImpact: Operational inefficiencies and potential compliance breaches
RiskDescription: Failure to utilize established methodologies for ML/TF risk assessments may result in

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Standardize risk assessment procedures", "2": "Implement peer reviews for asses
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 659:
RiskId: 1881
ComplianceId: 2535
RiskTitle: Increased Money Laundering Risk
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Failure to implement tailored AML/CFT measures based on risk assessments may lea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for staff on AML/CFT measures", "2": "
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 660:
RiskId: 1882

ComplianceId: 2536
RiskTitle: Non-Compliance with FATF Standards
Criticality: Medium
PossibleDamage: Regulatory sanctions, reputational damage, loss of business opportunities
Category: Compliance
RiskType: Current
BusinessImpact: Compliance, Operations
RiskDescription: Failure to develop and apply a framework for categorizing corridors in compliance witl
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on FATF standards for staff involved in corridor categorization", "
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 661:
RiskId: 1883
ComplianceId: 2539
RiskTitle: Inadequate Risk Assessment Due to Infrequent Meetings
Criticality: High
PossibleDamage: Increased financial crimes, regulatory fines, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, regulatory sanctions, and damage to reputation
RiskDescription: Infrequent meetings may result in outdated risk assessments and ineffective mitigatio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear meeting schedules and agendas", "2": "Implement virtual meeting
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 662:
RiskId: 1884
ComplianceId: 2540
RiskTitle: Delayed Response to Emerging Risks
Criticality: Medium
PossibleDamage: Financial losses, regulatory fines, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, regulatory sanctions, and damage to reputation
RiskDescription: Failure to promptly address emerging risks may lead to financial losses, regulatory fin
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a process for identifying and escalating emerging risks", "2": "Conduct a
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 663:
RiskId: 1885
ComplianceId: 2541
RiskTitle: False Identity Fraud Risk
Criticality: High
PossibleDamage: Financial losses and reputational damage due to fraudulent transactions

Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses and reputational damage
RiskDescription: Customers using false identities may engage in fraudulent activities, leading to financ
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust identity verification processes", "2": "Provide training to staff on
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 664:
RiskId: 1886
ComplianceId: 2542
RiskTitle: Beneficial Owner Non-Identification Risk
Criticality: Medium
PossibleDamage: Regulatory non-compliance and exposure to financial crimes
Category: Legal
RiskType: Inherent
BusinessImpact: Legal and compliance departments would face regulatory scrutiny and potential pena
RiskDescription: Failure to identify beneficial owners may result in regulatory non-compliance and expo
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement clear procedures for beneficial owner identification", "2": "Regularly up
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 665:
RiskId: 1887
ComplianceId: 2543
RiskTitle: Failure to Identify Suspicious Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal actions
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, damage to reputation
RiskDescription: Failure to identify suspicious transactions may result in the organization being used fo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance staff training on identifying suspicious transactions", "2": "Implement aut
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 666:
RiskId: 1888
ComplianceId: 2544
RiskTitle: Delay in Reporting Suspicious Transactions
Criticality: Medium
PossibleDamage: Financial losses, regulatory penalties, legal actions
Category: Operational
RiskType: Inherent
BusinessImpact: Legal implications, reputational damage
RiskDescription: Delay in reporting suspicious transactions to the FIU may result in missed opportunitie

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated reporting systems", "2": "Establish clear reporting protocols
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 667:
RiskId: 1889
ComplianceId: 2545
RiskTitle: Failure to Detect Suspicious Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, legal consequences
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, legal consequences, reputational damage
RiskDescription: Undetected suspicious transactions may lead to regulatory sanctions and financial los
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance transaction monitoring systems", "2": "Implement regular staff training o
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 668:
RiskId: 1890

ComplianceId: 2546
RiskTitle: Inadequate Risk Assessment Process
Criticality: High
PossibleDamage: Inadequate risk management, non-compliance with regulations
Category: Operational
RiskType: Inherent
BusinessImpact: Increased exposure to money laundering risks, regulatory fines
RiskDescription: Failure to conduct effective risk assessments may lead to regulatory non-compliance
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear risk assessment procedures", "2": "Engage key stakeholders in the
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 669:
RiskId: 1891
ComplianceId: 2547
RiskTitle: Inaccurate Data Collection on Trade and Investment Patterns
Criticality: High
PossibleDamage: Inaccurate data may lead to flawed risk assessments and regulatory non-compliance
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory penalties and reputational damage
RiskDescription: Failure to collect accurate data on trade and investment patterns may result in flawed
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement automated data collection processes", "2": "Regular training for design
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 670:
RiskId: 1892
ComplianceId: 2548
RiskTitle: Inadequate Analysis of Remittance Characteristics
Criticality: Medium
PossibleDamage: Overlooking key risk factors and vulnerabilities in remittance characteristics
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased ML/TF risks and regulatory scrutiny
RiskDescription: Failure to conduct thorough analysis of remittance characteristics may lead to overloo
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Utilize advanced statistical tools for data analysis", "2": "Regular training for analy
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 671:
RiskId: 1893
ComplianceId: 2549
RiskTitle: Increased Exposure to Financial Crimes
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage

Category: Compliance
RiskType: Inherent
BusinessImpact: Financial institutions' reputation, regulatory compliance, financial stability
RiskDescription: Failure to develop risk profiles for remittance corridors may lead to increased exposur
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update risk profiles based on new data", "2": "Implement en
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 672:
RiskId: 1894
ComplianceId: 2550
RiskTitle: Failure to Conduct Annual Threat Assessment
Criticality: High
PossibleDamage: Increased exposure to financial crimes and regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance failures, reputational damage, financial losses
RiskDescription: Failure to conduct the annual threat assessment may lead to unidentified threats and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement enhanced monitoring and surveillance measures", "2": "Conduct ad-ho
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 673:
RiskId: 1895
ComplianceId: 2551
RiskTitle: Failure to Review Threat and Vulnerability Assessment
Criticality: Medium
PossibleDamage: Outdated risk assessments and ineffective risk mitigation strategies
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance failures, financial losses
RiskDescription: Failure to review threat indicators and vulnerabilities in remittance corridors may lead
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement real-time monitoring tools", "2": "Conduct periodic reviews based on tra
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 674:
RiskId: 1896
ComplianceId: 2552
RiskTitle: Exceeding Monetary Thresholds
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Financial
RiskType: Current
BusinessImpact: Disruption to remittance operations, financial penalties, loss of customer trust
RiskDescription: Transactions exceeding established monetary thresholds pose a significant risk of fina

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of transactions against thresholds", "2": "Immediate escalation
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 675:
RiskId: 1897
ComplianceId: 2553
RiskTitle: Unrestricted High-Risk Activities
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Financial
RiskType: Current
BusinessImpact: Increased exposure to financial crimes, regulatory penalties, loss of customer trust
RiskDescription: Lack of restrictions on high-risk activities can lead to potential financial crimes and reg
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement transaction monitoring systems", "2": "Enforce strict approval processe
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 676:
RiskId: 1898

ComplianceId: 2554
RiskTitle: Misalignment in risk management strategies with AML/CFT authorities
Criticality: High
PossibleDamage: Potential regulatory penalties and reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Compliance department
RiskDescription: Failure to share CRA findings with AML/CFT authorities may result in regulatory non-c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication channels with AML/CFT authorities", "2": "Impleme
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 677:
RiskId: 1899
ComplianceId: 2555
RiskTitle: Failure to Verify Low-Risk Customer Identities
Criticality: High
PossibleDamage: Potential money laundering or terrorist financing activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial penalties, and reputational damage
RiskDescription: Failure to verify the identities of low-risk customers may result in facilitating illicit finan
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement robust automated identity verification processes", "2": "Regularly upda
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 678:
RiskId: 1900
ComplianceId: 2556
RiskTitle: Failure to Monitor Transactions of Low-Risk Customers
Criticality: High
PossibleDamage: Undetected money laundering or terrorist financing activities
Category: Compliance
RiskType: Inherent
BusinessImpact: Increased regulatory scrutiny, financial penalties, and reputational damage
RiskDescription: Failure to monitor transactions of low-risk customers may result in facilitating illicit fina
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 75.66
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust automated transaction monitoring systems", "2": "Regularly upd
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 679:
RiskId: 1901
ComplianceId: 2557
RiskTitle: Failure to Report Suspicious Transactions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of customer trust

Category: Operational
RiskType: Current
BusinessImpact: Potential legal consequences, financial losses, damage to reputation
RiskDescription: Failure to report suspicious transactions in a timely manner may lead to regulatory scr
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement real-time transaction monitoring systems", "2": "Provide ongoing trainin
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 680:
RiskId: 1902
ComplianceId: 2558
RiskTitle: Non-Compliance with Cross-Border Monitoring
Criticality: High
PossibleDamage: Regulatory penalties, legal action, reputational harm
Category: Operational
RiskType: Current
BusinessImpact: Legal consequences, financial losses, damage to reputation
RiskDescription: Failure to monitor cross-border transactions for suspicious activity may lead to violatio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement cross-border transaction monitoring systems", "2": "Provide specialized
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 681:
RiskId: 1903
ComplianceId: 2559
RiskTitle: Undetected Money Laundering Threats
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial institutions, regulatory bodies
RiskDescription: Failure to conduct annual comprehensive risk assessments may result in undetected
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on risk assessment methodologies", "2": "Utilization of advanced
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 682:
RiskId: 1904
ComplianceId: 2560
RiskTitle: Incomplete Risk Assessments
Criticality: Medium
PossibleDamage: Inadequate risk mitigation strategies, regulatory non-compliance
Category: Compliance
RiskType: Current
BusinessImpact: Financial institutions, regulatory bodies
RiskDescription: Failure to utilize both quantitative and qualitative data may result in incomplete risk as

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review of data sources for accuracy and relevance", "2": "Cross-validatio
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 683:
RiskId: 1905
ComplianceId: 2561
RiskTitle: Failure to Detect Suspicious Activities
Criticality: High
PossibleDamage: Undetected money laundering activities, regulatory fines, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Compliance departments within financial institutions
RiskDescription: Failure to detect suspicious activities in remittance corridors may lead to severe finan
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and calibrate monitoring systems", "2": "Provide ongoing trainin
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 684:
RiskId: 1906

ComplianceId: 2562
RiskTitle: Delayed Review of Suspicious Activities Reports
Criticality: Medium
PossibleDamage: Delayed detection of suspicious activities, regulatory non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: Compliance departments within financial institutions, designated regulatory authorities
RiskDescription: Delayed review of suspicious activities reports may lead to regulatory non-compliance
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear review protocols and timelines", "2": "Assign dedicated staff for rep
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 685:
RiskId: 1907
ComplianceId: 2563
RiskTitle: Ineffective Communication with Counter-Terrorism Authorities
Criticality: High
PossibleDamage: Delayed threat detection and increased vulnerability to terrorist financing activities
Category: Operational
RiskType: Inherent
BusinessImpact: Compliance, Risk Management, Intelligence Units
RiskDescription: Failure to establish effective communication protocols with counter-terrorism authoritie
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly review and update communication protocols", "2": "Conduct training ses
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 686:
RiskId: 1908
ComplianceId: 2564
RiskTitle: Inadequate Joint Assessments with Counter-Terrorism Authorities
Criticality: High
PossibleDamage: Overlooking critical threat indicators and potential terrorist financing activities
Category: Operational
RiskType: Inherent
BusinessImpact: Compliance, Risk Management, Intelligence Units
RiskDescription: Failure to conduct regular joint assessments with counter-terrorism authorities may le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a structured assessment framework for joint evaluations", "2": "Assign d
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 687:
RiskId: 1909
ComplianceId: 2565
RiskTitle: Failure to Monitor Remittance Flows
Criticality: High
PossibleDamage: Facilitating terrorist financing activities

Category: Compliance
RiskType: Inherent
BusinessImpact: All business units within the financial institution
RiskDescription: Failure to monitor remittance flows may result in undetected terrorist financing activitie
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced staff training on identifying suspicious transactions", "2": "Regular indep
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 688:
RiskId: 1910
ComplianceId: 2566
RiskTitle: Failure to Identify High-Risk Corridors
Criticality: High
PossibleDamage: Inadequate risk assessment and mitigation strategies
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance and Risk Assessment Team
RiskDescription: Failure to identify high-risk corridors may result in overlooking significant risks associa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct thorough data analysis to identify high-risk corridors", "2": "Engage with r
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 689:
RiskId: 1911
ComplianceId: 2567
RiskTitle: Delay in Stakeholder Consultations
Criticality: Medium
PossibleDamage: Impact on the quality and comprehensiveness of the CRA
Category: Compliance
RiskType: Inherent
BusinessImpact: Compliance and Risk Assessment Team, Stakeholders
RiskDescription: Delay in stakeholder consultations may result in insufficient input and feedback, affec
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Set clear milestones and deadlines for stakeholder engagement", "2": "Regularly
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 690:
RiskId: 1912
ComplianceId: 2568
RiskTitle: Inadequate Data Sharing Framework
Criticality: High
PossibleDamage: Incomplete risk assessments and inadequate risk mitigation strategies
Category: Operational
RiskType: Current
BusinessImpact: Delayed risk identification and response
RiskDescription: Failure to establish a cooperation framework for data sharing may lead to incomplete

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the cooperation framework", "2": "Provide training or
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 691:
RiskId: 1913
ComplianceId: 2569
RiskTitle: Lack of Formal Agreements
Criticality: Medium
PossibleDamage: Miscommunication, delays, and inefficiencies in the CRA process
Category: Operational
RiskType: Current
BusinessImpact: Operational inefficiencies, delays in risk assessment
RiskDescription: Failure to establish MOUs may result in miscommunication, delays, and inefficiencies
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update MOUs", "2": "Provide training on importance of MOU
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 692:
RiskId: 1914

ComplianceId: 2570
RiskTitle: Failure to Conduct Joint Risk Assessments
Criticality: High
PossibleDamage: Failure to identify and mitigate risks in the remittance corridor, leading to potential fi
Category: Operational
RiskType: Inherent
BusinessImpact: Increased exposure to money laundering and terrorist financing activities
RiskDescription: Not conducting joint risk assessments may result in overlooking critical risks and vuln
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear schedule for joint risk assessments and data sharing activities",
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 693:
RiskId: 1915
ComplianceId: 2571
RiskTitle: Inadequate Data Sharing
Criticality: High
PossibleDamage: Failure to share critical information may result in incomplete risk assessments and ir
Category: Operational
RiskType: Inherent
BusinessImpact: Increased exposure to money laundering and terrorist financing activities
RiskDescription: Lack of data sharing between countries may hinder the identification of cross-border r
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish secure data sharing protocols and agreements between countries", "2":

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 694:

RiskId: 1916

ComplianceId: 2572

RiskTitle: Incomplete Data Collection

Criticality: High

PossibleDamage: Inaccurate risk assessments and potential regulatory non-compliance

Category: Operational

RiskType: Inherent

BusinessImpact: Risk assessment accuracy and regulatory compliance may be compromised.

RiskDescription: Failure to collect relevant data before risk assessment may result in inaccurate risk ev

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear data collection timelines and responsibilities", "2": "Implement data

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 695:

RiskId: 1917

ComplianceId: 2573

RiskTitle: Outdated Data Review

Criticality: Medium

PossibleDamage: Incorrect risk assessments and potential compliance issues

Category: Operational
RiskType: Inherent
BusinessImpact: Risk assessment accuracy and regulatory compliance may be compromised.
RiskDescription: Failure to review data annually may result in outdated information being used for risk
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish annual data review processes", "2": "Implement data validation checks
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 696:
RiskId: 1918
ComplianceId: 2574
RiskTitle: Failure to Collect Quantitative Data
Criticality: High
PossibleDamage: Undetected suspicious activities, non-compliance penalties, reputational harm
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory scrutiny, damaged reputation
RiskDescription: Failure to collect quantitative data may result in overlooking suspicious activities and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated data collection tools and reporting systems", "2": "Regular
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 697:
RiskId: 1919
ComplianceId: 2575
RiskTitle: Ineffective AML/CFT Measures
Criticality: High
PossibleDamage: Increased risk of financial crimes in the remittance corridor
Category: Compliance
RiskType: Residual
BusinessImpact: Research teams, compliance officers
RiskDescription: Failure to conduct annual qualitative data collection may result in ineffective AML/CFT
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure designated teams are trained on data collection methods", "2": "Implemen
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 698:
RiskId: 1920
ComplianceId: 2576
RiskTitle: Inaccurate Proceeds of Crime Analysis Report
Criticality: High
PossibleDamage: Potential regulatory fines, reputational damage, increased money laundering risk ex
Category: Compliance
RiskType: Current
BusinessImpact: Financial institutions may face penalties, loss of customer trust, and increased regula
RiskDescription: Inaccurate POC analysis reports can lead to misinformed decision-making, increased

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data validation processes to ensure accuracy of collected inform
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 699:
RiskId: 1921
ComplianceId: 2577
RiskTitle: Outdated Proceeds of Crime Analysis Review
Criticality: Medium
PossibleDamage: Increased exposure to money laundering risks, regulatory fines, reputational damag
Category: Compliance
RiskType: Current
BusinessImpact: Financial institutions may face regulatory penalties, loss of credibility, and heightened
RiskDescription: Outdated POC analysis reviews can lead to ineffective risk mitigation strategies, regu
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated alerts for significant changes in crime patterns for timely re
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 700:
RiskId: 1922

ComplianceId: 2578
RiskTitle: Increased Money Laundering Risk in Remittance Corridors
Criticality: High
PossibleDamage: Increased exposure to money laundering activities and regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Risk management and compliance functions would be significantly impacted
RiskDescription: Failure to accurately assess ML risks in remittance corridors could lead to increased e
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on ML risk assessment methodology", "2": "Independent audits o
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 701:
RiskId: 1923
ComplianceId: 2579
RiskTitle: Failure to Establish Formal Channels for Information Sharing
Criticality: High
PossibleDamage: Delayed threat assessment, ineffective collaboration
Category: Operational
RiskType: Inherent
BusinessImpact: Compromised compliance monitoring, regulatory adherence, threat assessment accu
RiskDescription: Unauthorized access to sensitive data, miscommunication leading to incorrect threat a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update and maintain the secure platform", "2": "Provide training on platf

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 702:

RiskId: 1924

ComplianceId: 2580

RiskTitle: Lack of Regular Workshops for Enhanced Cooperation

Criticality: Medium

PossibleDamage: Outdated threat assessments, reduced cooperation

Category: Operational

RiskType: Inherent

BusinessImpact: Collaboration effectiveness, threat assessment accuracy compromised

RiskDescription: Miscommunication, lack of stakeholder engagement, outdated threat assessments

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Schedule workshops in advance and ensure participation", "2": "Provide relevant

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 703:

RiskId: 1925

ComplianceId: 2581

RiskTitle: Failure to Conduct Annual Threat Analysis

Criticality: High

PossibleDamage: Increased exposure to terrorist financing activities and regulatory penalties

Category: Compliance
RiskType: Current
BusinessImpact: Non-compliance may lead to financial losses, regulatory fines, and damage to reputat
RiskDescription: Failure to conduct the annual threat analysis may result in overlooking potential terror
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on threat analysis techniques", "2": "Enhanced monitoring of pay
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 704:
RiskId: 1926
ComplianceId: 2582
RiskTitle: Delay in Assessing Threat Landscape Changes
Criticality: Medium
PossibleDamage: Vulnerabilities to new terrorist financing schemes
Category: Compliance
RiskType: Current
BusinessImpact: May lead to regulatory fines, reputational damage, and operational disruptions
RiskDescription: Failure to promptly assess changes in the threat landscape may expose the organizat
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Real-time monitoring of threat intelligence sources", "2": "Establishing rapid respo
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 705:
RiskId: 1927
ComplianceId: 2583
RiskTitle: Ineffective Communication with Authorities
Criticality: High
PossibleDamage: Delayed threat assessments and increased risk of terrorist financing activities going
Category: Operational
RiskType: Inherent
BusinessImpact: Direct impact on compliance and risk management functions
RiskDescription: Failure to establish formal communication channels with authorities may result in dela
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update communication protocols", "2": "Conduct training ses
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 706:
RiskId: 1928
ComplianceId: 2584
RiskTitle: Lack of Quarterly Collaboration Meetings
Criticality: Medium
PossibleDamage: Lack of updated threat information and ineffective threat assessments
Category: Operational
RiskType: Inherent
BusinessImpact: Direct impact on compliance and risk management functions
RiskDescription: Failure to hold quarterly collaboration meetings may result in outdated threat informat

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a meeting schedule for the year in advance", "2": "Prepare agenda item
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 707:
RiskId: 1929
ComplianceId: 2585
RiskTitle: Failure to Identify High-Risk Corridors
Criticality: High
PossibleDamage: Inadequate risk assessment and mitigation, potential financial losses, regulatory per
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, regulatory non-compliance
RiskDescription: Failure to identify high-risk corridors may result in inadequate risk assessment, leadin
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular risk assessments to identify emerging high-risk corridors", "2": "I
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 708:
RiskId: 1930

ComplianceId: 2586
RiskTitle: Failure to Conduct Periodic Reviews of Corridors
Criticality: Medium
PossibleDamage: Outdated risk assessments, ineffective risk mitigation strategies, potential exposure
Category: Operational
RiskType: Inherent
BusinessImpact: Ineffective risk management, potential exposure to risks
RiskDescription: Failure to conduct periodic reviews may result in outdated risk assessments, leading t
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a structured review process with defined criteria for reassessment", "2":
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 709:
RiskId: 1931
ComplianceId: 2587
RiskTitle: Inadequate Risk Assessment Methodology Implementation
Criticality: High
PossibleDamage: Increased exposure to ML/TF risks
Category: Compliance
RiskType: Current
BusinessImpact: Risk assessment teams, regulatory authorities, and financial institutions
RiskDescription: Failure to implement the standardized risk assessment methodology may lead to inco
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Provide training to designated risk assessment teams on the standardized metho

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 710:

RiskId: 1932

ComplianceId: 2588

RiskTitle: Inadequate Information Sharing for NRAs and CRAs

Criticality: High

PossibleDamage: Incomplete risk assessments, increased ML/TF risks, and compromised effectivenes

Category: Operational

RiskType: Current

BusinessImpact: Delays in identifying and addressing ML/TF risks, potential regulatory non-compliance

RiskDescription: Lack of formal agreements for information sharing may hinder the effectiveness of risk

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly review and update the memoranda of understanding", "2": "Provide trai

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 711:

RiskId: 1933

ComplianceId: 2589

RiskTitle: Outdated NRA Risk Assessments

Criticality: High

PossibleDamage: Ineffective AML/CFT measures, increased exposure to ML/TF risks

Category: Compliance
RiskType: Current
BusinessImpact: Compromised national AML/CFT efforts, potential regulatory sanctions, reputational d
RiskDescription: Failure to update the NRA may result in outdated risk assessments that do not accura
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a structured review process that includes data collection, analysis, and
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 712:
RiskId: 1934
ComplianceId: 2590
RiskTitle: Incomplete Data Collection
Criticality: High
PossibleDamage: Flawed risk assessments and decision-making processes
Category: Operational
RiskType: Inherent
BusinessImpact: May lead to regulatory non-compliance, financial losses, or reputational damage
RiskDescription: Incomplete or inaccurate data collection may result in flawed risk assessments and de
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on data collection tools and methodologies", "2": "Periodic audits
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 713:
RiskId: 1935
ComplianceId: 2591
RiskTitle: Outdated Data Collection
Criticality: Medium
PossibleDamage: Incorrect risk assessments and ineffective decision-making processes
Category: Operational
RiskType: Inherent
BusinessImpact: May lead to incorrect risk assessments, regulatory non-compliance, or financial losse
RiskDescription: Outdated data collection may result in incorrect risk assessments and ineffective deci
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish automated data update reminders", "2": "Regular review of data source
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 714:
RiskId: 1936
ComplianceId: 2592
RiskTitle: Inadequate Expert Involvement
Criticality: High
PossibleDamage: Inaccurate risk assessments and inadequate mitigation strategies
Category: Operational
RiskType: Inherent
BusinessImpact: Quality of risk assessments, compliance with regulations, reputation
RiskDescription: Failure to engage qualified experts may result in inaccurate risk assessments and ina

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear selection criteria for experts", "2": "Define roles and responsibilities
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 715:
RiskId: 1937
ComplianceId: 2593
RiskTitle: Lack of Expert Engagement Framework
Criticality: Medium
PossibleDamage: Confusion, inefficiency, and inconsistent expert involvement
Category: Operational
RiskType: Inherent
BusinessImpact: Risk assessment efficiency, quality, compliance
RiskDescription: The absence of a structured framework for expert engagement may lead to confusion
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Define clear selection criteria for experts", "2": "Document roles and responsibilitie
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 716:
RiskId: 1938

ComplianceId: 2594
RiskTitle: Inadequate Stakeholder Engagement and Data Sharing
Criticality: High
PossibleDamage: Incomplete or delayed risk assessments, inadequate risk mitigation strategies
Category: Operational
RiskType: Current
BusinessImpact: Risk assessment process, decision-making, regulatory compliance
RiskDescription: Failure to establish a formal framework for stakeholder engagement and data sharing
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on stakeholder engagement and data s
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 717:
RiskId: 1939
ComplianceId: 2595
RiskTitle: Lack of Coordination in Risk Assessment
Criticality: High
PossibleDamage: Delays in risk assessment process, errors in risk identification
Category: Operational
RiskType: Current
BusinessImpact: All business units involved in risk assessment process
RiskDescription: Lack of clear coordination between lead agency and project team may result in delays
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular project team meetings to discuss progress and challenges", "2": "Provide

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 718:

RiskId: 1940

ComplianceId: 2596

RiskTitle: Unclear Project Team Roles and Responsibilities

Criticality: Medium

PossibleDamage: Confusion and inefficiencies in project execution

Category: Operational

RiskType: Current

BusinessImpact: Project team members from relevant stakeholder organizations

RiskDescription: Unclear roles and responsibilities within the project team may lead to confusion in pro

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regular review of project charter to ensure alignment with project goals", "2": "Pro

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 719:

RiskId: 1941

ComplianceId: 2597

RiskTitle: Failure to Identify High-Risk Remittance Corridors

Criticality: High

PossibleDamage: Increased exposure to money laundering, terrorist financing, and other illicit activities

Category: Compliance
RiskType: Inherent
BusinessImpact: Regulatory sanctions, loss of credibility
RiskDescription: Failure to identify high-risk remittance corridors may lead to inadequate risk mitigation
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular training on identifying high-risk corridors", "2": "Implement enhan
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 720:
RiskId: 1942
ComplianceId: 2598
RiskTitle: Failure to Identify Emerging Risks for Remittance Corridors
Criticality: High
PossibleDamage: Regulatory non-compliance, financial losses, reputational harm
Category: Compliance
RiskType: Inherent
BusinessImpact: Regulatory sanctions, financial losses, reputational damage
RiskDescription: Failure to identify and address emerging risks in remittance corridors may result in reg
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a dedicated team for monitoring emerging risks", "2": "Engage with indu
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 721:
RiskId: 1943
ComplianceId: 2599
RiskTitle: Misalignment of CRA Directionality
Criticality: High
PossibleDamage: Misaligned risk assessments, ineffective risk management
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate risk assessments, regulatory non-compliance
RiskDescription: Incorrect determination of CRA directionality leading to misaligned risk assessments a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and updates on data analysis techniques", "2": "Cross-validation
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 722:
RiskId: 1944
ComplianceId: 2600
RiskTitle: Unidentified Risks in Remittance Corridors
Criticality: High
PossibleDamage: Regulatory penalties, financial losses
Category: Compliance
RiskType: Current
BusinessImpact: Regulatory fines, reputational damage
RiskDescription: Failure to conduct a comprehensive assessment may result in unidentified risks in rer

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for assessment teams on updated assessment techniques", "2":
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 723:
RiskId: 1945
ComplianceId: 2601
RiskTitle: Legal Consequences for Non-Compliance
Criticality: High
PossibleDamage: Legal fines and reputational damage
Category: Legal
RiskType: Inherent
BusinessImpact: Legal actions may affect the organization's operations and reputation
RiskDescription: Failure to obtain explicit consent may result in legal actions against the organization
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular legal compliance reviews", "2": "Engage legal counsel for consent manag
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 724:
RiskId: 1946

ComplianceId: 2602
RiskTitle: Data Encryption Vulnerability
Criticality: High
PossibleDamage: Data breaches and regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data and damage to organizational reputation
RiskDescription: Failure to encrypt personal data may result in unauthorized access and data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly audit encryption practices", "2": "Implement data loss prevention tools",
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 725:
RiskId: 1947
ComplianceId: 2603
RiskTitle: Access Control Vulnerability
Criticality: Medium
PossibleDamage: Data breaches and privacy violations
Category: Operational
RiskType: Current
BusinessImpact: Unauthorized access to sensitive data and potential legal consequences
RiskDescription: Inadequate access controls may lead to unauthorized users gaining access to person
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly review access permissions", "2": "Implement two-factor authentication f

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 726:

RiskId: 1948

ComplianceId: 2604

RiskTitle: Unauthorized Access to Outdated Personal Data

Criticality: High

PossibleDamage: Risk of data breaches, privacy violations, and legal consequences.

Category: Compliance

RiskType: Current

BusinessImpact: Potential loss of trust from customers, financial losses from legal penalties.

RiskDescription: Outdated personal data may still be accessible and pose a risk of data breaches or pr

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly review and update data retention schedules", "2": "Implement encryptio

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 727:

RiskId: 1949

ComplianceId: 2605

RiskTitle: Delayed Data Breach Notification

Criticality: High

PossibleDamage: Legal penalties, reputational damage, loss of customer trust

Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, regulatory fines
RiskDescription: Failure to notify relevant parties immediately upon data breach discovery
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear notification protocols", "2": "Regular training for incident response
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 728:
RiskId: 1950
ComplianceId: 2606
RiskTitle: Misinterpretation of Personal and Domestic Activities
Criticality: High
PossibleDamage: Unauthorized data processing leading to compliance violations
Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal consequences and reputational damage
RiskDescription: Unclear definitions of personal and domestic activities could result in employees proc
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on personal and domestic activities definitions", "2": "Clear comm
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 729:
RiskId: 1951
ComplianceId: 2607
RiskTitle: Non-Compliance with Access Request Process
Criticality: High
PossibleDamage: Legal actions, fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Legal consequences and reputational damage
RiskDescription: Failure to establish a formal process for access requests may result in delayed or non
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on the access request process", "2": "Regular audits to e
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 730:
RiskId: 1952
ComplianceId: 2608
RiskTitle: Incomplete or Inaccurate Information in Access Requests
Criticality: Medium
PossibleDamage: Non-compliance, legal actions, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Legal consequences and reputational damage
RiskDescription: Failure to utilize a standardized form may result in incomplete or inaccurate informatio

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Training for staff on completing the standardized form accurately", "2": "Regular re
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 731:
RiskId: 1953
ComplianceId: 2609
RiskTitle: Unauthorized Data Disclosure Risk
Criticality: High
PossibleDamage: Unauthorized disclosure of personal data leading to privacy breaches
Category: Compliance
RiskType: Current
BusinessImpact: All departments handling personal data would be impacted
RiskDescription: Inaccurate list of third parties may result in unauthorized disclosure of personal data, v
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on data handling procedures", "2": "Encryption of sensitive data i
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 732:
RiskId: 1954

ComplianceId: 2610
RiskTitle: Outdated List Risk
Criticality: Medium
PossibleDamage: Outdated list leading to incorrect responses to access requests
Category: Compliance
RiskType: Current
BusinessImpact: Data Protection Officer (DPO) efficiency and accuracy would be impacted
RiskDescription: An outdated list of third parties may result in incorrect responses to access requests,
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated reminders for quarterly reviews", "2": "Regular communication with de
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 733:
RiskId: 1955
ComplianceId: 2611
RiskTitle: Delayed Response to Access Requests
Criticality: High
PossibleDamage: Legal penalties and reputational harm
Category: Compliance
RiskType: Current
BusinessImpact: Customer dissatisfaction and loss of trust
RiskDescription: Failure to respond to access requests within the required timeframe may result in lega
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear escalation procedures for delayed responses", "2": "Regular monit

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 734:

RiskId: 1956

ComplianceId: 2612

RiskTitle: Inconsistent Response Format

Criticality: Medium

PossibleDamage: Customer dissatisfaction and operational inefficiencies

Category: Operational

RiskType: Current

BusinessImpact: Increased customer complaints and potential errors in information provided

RiskDescription: Failure to use standardized response templates may lead to inconsistencies in inform

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Provide training on template usage and content requirements", "2": "Implement qu

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 735:

RiskId: 1957

ComplianceId: 2613

RiskTitle: Inaccurate Data Validation

Criticality: High

PossibleDamage: Inaccurate personal data affecting decision-making processes

Category: Operational
RiskType: Residual
BusinessImpact: Incorrect decisions, regulatory non-compliance, reputational damage
RiskDescription: Failure to accurately validate personal data through automated tools could result in in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and maintain automated validation tools", "2": "Provide training t
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 736:
RiskId: 1958
ComplianceId: 2614
RiskTitle: Outdated Data Verification
Criticality: Medium
PossibleDamage: Outdated personal data affecting decision-making processes
Category: Operational
RiskType: Residual
BusinessImpact: Incorrect decisions, regulatory non-compliance, reputational harm
RiskDescription: Failure to conduct annual data verification processes could result in outdated persona
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a schedule for annual data verification processes", "2": "Implement data
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 737:
RiskId: 1959
ComplianceId: 2615
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data exposure, legal liabilities
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties
RiskDescription: Unauthorized access to personal data leading to breaches and legal consequences
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for sensitive data", "2": "Enforce strict access controls", "3":
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 738:
RiskId: 1960
ComplianceId: 2616
RiskTitle: Data Misclassification Risk
Criticality: Medium
PossibleDamage: Incorrect data handling, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate data processing, regulatory fines
RiskDescription: Misclassification of personal data leading to incorrect handling and potential complian

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update data classification criteria", "2": "Implement data vali
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 739:
RiskId: 1961
ComplianceId: 2617
RiskTitle: Failure to Notify Individuals of Delay in Access Request Response
Criticality: High
PossibleDamage: Loss of trust, legal implications, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions and legal consequences
RiskDescription: Failure to notify individuals of delays in access request responses may result in legal
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of response timelines", "2": "Establishing clear escalation proc
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 740:
RiskId: 1962

ComplianceId: 2618
RiskTitle: Unauthorized Disclosure of Deceased Individuals' Data
Criticality: High
PossibleDamage: Legal actions, reputational damage, loss of trust
Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal penalties, reputational damage, loss of customer trust
RiskDescription: Failure to notify individuals or representatives may result in unauthorized disclosure o
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust notification process with clear guidelines and timelines", "2": "
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 741:
RiskId: 1963
ComplianceId: 2619
RiskTitle: Legal Action Due to Lack of Consent
Criticality: High
PossibleDamage: Legal costs, fines, and reputational damage
Category: Legal
RiskType: Current
BusinessImpact: Potential legal actions and financial penalties
RiskDescription: Failure to obtain explicit consent may result in legal actions from individuals whose da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on consent management procedures", "2": "Periodic audits to ens

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 742:

RiskId: 1964

ComplianceId: 2620

RiskTitle: Disputes Over Consent Validity

Criticality: Medium

PossibleDamage: Operational disruptions and legal challenges

Category: Operational

RiskType: Current

BusinessImpact: Operational disruptions and potential legal disputes

RiskDescription: Inconsistencies in consent forms may lead to disputes over the validity of consent obt

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Training on the proper use of standardized consent forms", "2": "Regular review o

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 743:

RiskId: 1965

ComplianceId: 2621

RiskTitle: Data Breach Risk

Criticality: High

PossibleDamage: Legal consequences, reputational damage

Category: Compliance
RiskType: Current
BusinessImpact: All business units handling personal data
RiskDescription: Unauthorized access to personal data due to lack of data minimization practices
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review data collection practices", "2": "Implement anonymization metho
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 744:
RiskId: 1966
ComplianceId: 2622
RiskTitle: Non-Compliance Risk
Criticality: Medium
PossibleDamage: Data breaches, regulatory fines
Category: Compliance
RiskType: Current
BusinessImpact: All business units handling personal data
RiskDescription: Failure to regularly review data collection practices leading to non-compliance with da
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement regular audits of data collection practices", "2": "Provide training on an
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 745:
RiskId: 1967
ComplianceId: 2625
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data exposure, reputational damage, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, loss of trust from stakeholders
RiskDescription: Risk of unauthorized access to personal data by third-party service providers due to i
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong data protection agreements", "2": "Regularly audit service provi
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 746:
RiskId: 1968
ComplianceId: 2626
RiskTitle: Lack of Data Protection Policy Notification
Criticality: High
PossibleDamage: Non-compliance penalties, loss of trust, legal actions
Category: Compliance
RiskType: Current
BusinessImpact: All departments handling personal data
RiskDescription: Failure to notify individuals about the Data Protection Policy may result in legal conse

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Include notification in privacy statements", "2": "Train staff to inform individuals ab
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 747:
RiskId: 1969
ComplianceId: 2627
RiskTitle: Outdated Data Protection Policy
Criticality: Medium
PossibleDamage: Non-compliance, ineffective data protection
Category: Compliance
RiskType: Current
BusinessImpact: Data Protection Officer (DPO)
RiskDescription: An outdated Data Protection Policy may not align with current data protection regulati
RiskLikelihood: 5
RiskImpact: 8
RiskExposureRating: 40
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a review schedule", "2": "Engage stakeholders in the review process", "
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 748:
RiskId: 1970

ComplianceId: 2628
RiskTitle: Lack of Informed Consent
Criticality: High
PossibleDamage: Loss of trust, legal fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: All departments involved in data collection
RiskDescription: Failure to inform individuals of data collection purposes may result in unauthorized us
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on data collection practices", "2": "Implementing clear da
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 749:
RiskId: 1971
ComplianceId: 2629
RiskTitle: Misinterpretation of Deemed Consent
Criticality: Medium
PossibleDamage: Unauthorized data usage, legal consequences
Category: Compliance
RiskType: Inherent
BusinessImpact: Responsible department (e.g., Customer Service)
RiskDescription: Failure to correctly identify deemed consent situations may lead to unauthorized use
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regular training sessions on recognizing deemed consent situations", "2": "Provid
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 750:
RiskId: 1972
ComplianceId: 2630
RiskTitle: Unauthorized Data Sharing
Criticality: High
PossibleDamage: Exposure of sensitive personal data, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, legal liabilities
RiskDescription: Unauthorized sharing of personal data with third parties due to lack of documentation
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls for data sharing systems", "2": "Regularly review and u
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 751:
RiskId: 1973
ComplianceId: 2631
RiskTitle: Contractual Breaches
Criticality: Medium
PossibleDamage: Legal disputes, financial penalties

Category: Legal
RiskType: Current
BusinessImpact: Reputational damage, financial losses
RiskDescription: Failure to include deemed consent provisions in contracts leading to breaches of cont
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish contract review processes", "2": "Provide training on contractual require
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 752:
RiskId: 1974
ComplianceId: 2634
RiskTitle: Unauthorized Data Processing Risk
Criticality: High
PossibleDamage: Data breaches, loss of customer trust, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Unauthorized data processing may lead to data breaches, loss of customer trust, and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict data collection procedures", "2": "Regularly review and update as
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 753:
RiskId: 1975
ComplianceId: 2635
RiskTitle: Documentation Non-Compliance Risk
Criticality: Medium
PossibleDamage: Legal implications, fines, reputational damage
Category: Legal
RiskType: Inherent
BusinessImpact: Legal consequences, financial losses, reputational damage
RiskDescription: Lack of documentation may result in non-compliance with PDPA, legal implications, fi
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement robust documentation procedures", "2": "Regularly audit and review do
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 754:
RiskId: 1976
ComplianceId: 2636
RiskTitle: Failure to Notify Individuals of Data Collection Intentions
Criticality: High
PossibleDamage: Legal penalties, loss of customer trust, and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Loss of customer trust, potential lawsuits, and negative impact on brand reputation
RiskDescription: Not providing clear notifications to individuals about data collection intentions can lea

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure compliance", "2": "Training for staff on notification requir
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 755:
RiskId: 1977
ComplianceId: 2637
RiskTitle: Lack of Clarity in Notification Emails
Criticality: High
PossibleDamage: Legal consequences and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal costs, loss of customer trust.
RiskDescription: Failure to provide clear information in notification emails may result in individuals not u
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update notification email templates", "2": "Conduct audits of
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 756:
RiskId: 1978

ComplianceId: 2638
RiskTitle: Late Notification Delivery
Criticality: Medium
PossibleDamage: Legal penalties and loss of trust
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal costs, negative public perception.
RiskDescription: Sending notifications less than 10 days before data disclosure may not provide indivi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate notification scheduling to ensure timely delivery", "2": "Establish escala
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 757:
RiskId: 1979
ComplianceId: 2639
RiskTitle: Failure to Provide Mechanism for Consent Withdrawal
Criticality: High
PossibleDamage: Non-compliance with data protection regulations and loss of customer trust
Category: Compliance
RiskType: Residual
BusinessImpact: Legal actions, reputational damage, loss of customer trust
RiskDescription: If organizations fail to provide a mechanism for consent withdrawal, individuals may ta
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication of the consent withdrawal process to individuals", "2
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 758:
RiskId: 1980
ComplianceId: 2640
RiskTitle: Delay in Processing Consent Withdrawal Requests
Criticality: Medium
PossibleDamage: Legal non-compliance and customer dissatisfaction
Category: Operational
RiskType: Residual
BusinessImpact: Legal actions, customer dissatisfaction
RiskDescription: If organizations delay in processing consent withdrawal requests, they may face legal
RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated tracking system for consent withdrawal requests", "2": "Allo
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 759:
RiskId: 1981
ComplianceId: 2641
RiskTitle: Uninformed Consent Risk
Criticality: High
PossibleDamage: Potential privacy violations and legal consequences

Category: Compliance
RiskType: Residual
BusinessImpact: Data handling processes and reputation may be compromised.
RiskDescription: Individuals may provide consent without understanding the purpose of data collection
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training to personnel on effective communication of data collection purpos
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 760:
RiskId: 1982
ComplianceId: 2642
RiskTitle: Unauthorized Data Processing Risk
Criticality: Medium
PossibleDamage: Unauthorized processing of personal data and non-compliance with regulations
Category: Legal
RiskType: Residual
BusinessImpact: Potential financial penalties and reputational damage
RiskDescription: Data collection activities initiated without obtaining prior consent may lead to unautho
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated consent tracking systems to ensure timely consent acquisit
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 761:
RiskId: 1983
ComplianceId: 2643
RiskTitle: Failure to Provide Access to Personal Data
Criticality: High
PossibleDamage: Legal penalties, reputational damage, loss of customer trust
Category: Operational
RiskType: Current
BusinessImpact: Potential legal costs, loss of customers, damage to reputation
RiskDescription: Failure to provide access to personal data as required by the PDPA may lead to legal
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on handling access requests", "2": "Regular audits to ens
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 762:
RiskId: 1984
ComplianceId: 2644
RiskTitle: Lack of Data Protection Officer Oversight
Criticality: Medium
PossibleDamage: Non-compliance with the PDPA, potential data breaches, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Potential fines, damage to reputation, data breaches
RiskDescription: Lack of oversight by the DPO may result in non-compliance with the PDPA, potential

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular reporting to senior management on compliance status", "2": "Training for
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 763:
RiskId: 1985
ComplianceId: 2645
RiskTitle: Unauthorized Access to Personal Data
Criticality: High
PossibleDamage: Privacy breaches, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, legal penalties
RiskDescription: Unauthorized access to personal data can lead to privacy breaches, legal consequen
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication measures for access requests", "2": "Regularly r
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 764:
RiskId: 1986

ComplianceId: 2646
RiskTitle: Delayed Processing of Access Requests
Criticality: Medium
PossibleDamage: Legal non-compliance, customer dissatisfaction
Category: Operational
RiskType: Current
BusinessImpact: Customer dissatisfaction, legal penalties
RiskDescription: Delayed processing of access requests can lead to legal non-compliance, customer d
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear escalation procedures for delayed requests", "2": "Regularly monit
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 765:
RiskId: 1987
ComplianceId: 2647
RiskTitle: Unauthorized Disclosure Risk
Criticality: High
PossibleDamage: Legal consequences and reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal action and loss of trust from stakeholders
RiskDescription: Failure to properly evaluate and manage disclosure requests could result in unauthori
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear criteria for evaluating disclosure requests", "2": "Regularly review a

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 766:

RiskId: 1988

ComplianceId: 2648

RiskTitle: Documentation Failure Risk

Criticality: Medium

PossibleDamage: Disputes over handling of personal data

Category: Compliance

RiskType: Residual

BusinessImpact: Legal disputes and challenges in defending actions

RiskDescription: Lack of proper documentation of disclosure requests could lead to disputes over the h

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement a standardized documentation process for all disclosure requests", "2"

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 767:

RiskId: 1989

ComplianceId: 2649

RiskTitle: Non-compliance with Data Protection Regulations

Criticality: High

PossibleDamage: Legal fines, reputational damage, loss of customer trust

Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal and financial consequences
RiskDescription: Failure to conduct bi-annual assessments may result in non-compliance with data pro
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a reminder system for bi-annual assessments", "2": "Provide training o
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 768:
RiskId: 1990
ComplianceId: 2650
RiskTitle: Privacy Violations due to Inappropriate Data Collection Methods
Criticality: Medium
PossibleDamage: Legal fines, reputational damage, loss of customer trust
Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal and financial consequences
RiskDescription: Failure to review data collection methods against reasonableness standards may resu
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide training on appropriate data collection methods", "2": "Implement regular
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 769:
RiskId: 1991
ComplianceId: 2651
RiskTitle: Failure to Notify Individuals of Consequences
Criticality: High
PossibleDamage: Legal disputes, loss of trust, financial penalties
Category: Compliance
RiskType: Current
BusinessImpact: Legal and reputational damage
RiskDescription: Failure to notify individuals of consequences of withdrawal of consent may result in le
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication protocols for data protection officers", "2": "Regula
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 770:
RiskId: 1992
ComplianceId: 2652
RiskTitle: Unauthorized Data Processing
Criticality: High
PossibleDamage: Legal and reputational consequences
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal penalties, loss of customer trust
RiskDescription: Continued data processing activities after withdrawal of consent could lead to unautho

RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Immediate cessation of data processing upon receipt of withdrawal notice", "2": "F
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 771:
RiskId: 1993
ComplianceId: 2653
RiskTitle: Unauthorized Data Processing by Intermediaries
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal consequences, financial penalties, loss of customer trust
RiskDescription: Failure to notify data intermediaries of consent withdrawal may result in unauthorized
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated notification systems for efficient communication", "2": "Regu
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 772:
RiskId: 1994

ComplianceId: 2654
RiskTitle: Inaccurate Data Collection Records
Criticality: High
PossibleDamage: Legal fines, reputational damage, loss of customer trust.
Category: Compliance
RiskType: Current
BusinessImpact: Operational disruptions, legal liabilities, loss of business opportunities.
RiskDescription: Failure to maintain accurate data collection records can result in legal non-compliance
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular data collection training for staff", "2": "Periodic audits of data collection re
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 773:
RiskId: 1995
ComplianceId: 2655
RiskTitle: Unauthorized Access to Data Disclosure Records
Criticality: Medium
PossibleDamage: Data breaches, legal repercussions, loss of trust.
Category: Compliance
RiskType: Current
BusinessImpact: Data confidentiality breaches, legal liabilities, reputational damage.
RiskDescription: Inadequate storage of data disclosure records can lead to unauthorized access, data
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement encryption measures for stored data disclosure records", "2": "Restrict
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 774:
RiskId: 1996
ComplianceId: 2656
RiskTitle: Unauthorized Disclosure of Personal Data
Criticality: High
PossibleDamage: Loss of customer trust, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Potential legal and financial implications
RiskDescription: Misclassification of personal data may lead to unauthorized disclosure, resulting in re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement data access controls", "2": "Regularly review and update data classific
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 775:
RiskId: 1997
ComplianceId: 2657
RiskTitle: Outdated Data Availability Checklist
Criticality: Medium
PossibleDamage: Inaccurate classification of personal data

Category: Operational
RiskType: Residual
BusinessImpact: Potential data breaches and regulatory non-compliance
RiskDescription: Failure to update the data availability checklist annually may result in misclassification
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Schedule annual review of checklist", "2": "Involve key stakeholders in the review
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 776:
RiskId: 1998
ComplianceId: 2658
RiskTitle: Non-Compliance with Notice Display
Criticality: High
PossibleDamage: Legal fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Legal consequences, loss of trust
RiskDescription: Failure to display notices may lead to legal non-compliance issues and damage to the
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure compliance", "2": "Training for staff on notice requiremer
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 777:
RiskId: 1999
ComplianceId: 2659
RiskTitle: Ineffective Online Notice Design
Criticality: Medium
PossibleDamage: Loss of trust, legal repercussions
Category: Compliance
RiskType: Current
BusinessImpact: Loss of customer trust, legal consequences
RiskDescription: Poorly designed online notices may lead to individuals misunderstanding data collecti
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "User testing for notice effectiveness", "2": "Regular updates based on user feedba
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 778:
RiskId: 2000
ComplianceId: 2660
RiskTitle: Failure to Obtain Explicit Consent
Criticality: High
PossibleDamage: Legal penalties and reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Legal disputes and loss of trust
RiskDescription: Individuals may challenge the organization's data collection practices, leading to legal

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Train staff on obtaining explicit consent", "2": "Regularly review and update conse
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 779:
RiskId: 2001
ComplianceId: 2661
RiskTitle: Unclear Responsibility for Consent Management
Criticality: Medium
PossibleDamage: Oversight and non-compliance
Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal consequences and regulatory fines
RiskDescription: Lack of clear responsibility may lead to oversight in obtaining consent, resulting in no
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Define clear roles and responsibilities for consent management", "2": "Provide tra
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 780:
RiskId: 2002

ComplianceId: 2662
RiskTitle: Lack of Clear Notification
Criticality: High
PossibleDamage: Privacy concerns, legal issues, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Legal investigations, reputational harm
RiskDescription: Failure to provide clear notifications may result in individuals being unaware of data c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear and concise language in notifications", "2": "Provide examples to hel
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 781:
RiskId: 2003
ComplianceId: 2663
RiskTitle: Late or Absent Notifications
Criticality: Medium
PossibleDamage: Privacy concerns, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Reputational harm, privacy complaints
RiskDescription: Late or absent notifications may prevent individuals from making informed decisions a
RiskLikelihood: 5
RiskImpact: 8
RiskExposureRating: 40
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish a notification timeline for all events", "2": "Implement automated notifica
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 782:
RiskId: 2004
ComplianceId: 2664
RiskTitle: Failure to Obtain Explicit Consent
Criticality: High
PossibleDamage: Legal penalties, loss of trust, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: All departments involved in data collection activities
RiskDescription: Failure to obtain explicit consent may result in legal non-compliance, loss of trust from
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for staff on obtaining explicit consent", "2": "Regular aud
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 783:
RiskId: 2005
ComplianceId: 2665
RiskTitle: Lack of DPO Oversight
Criticality: Medium
PossibleDamage: Inconsistent application of consent management process, potential non-compliance

Category: Operational
RiskType: Current
BusinessImpact: Data Protection Office
RiskDescription: Lack of oversight by the DPO may result in inconsistent application of the consent ma
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular reporting to senior management on consent management activities", "2":
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 784:
RiskId: 2006
ComplianceId: 2666
RiskTitle: Delayed Data Breach Notification
Criticality: High
PossibleDamage: Increased data exposure and regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: All business units handling personal data
RiskDescription: Failure to promptly notify affected parties and regulatory authorities of a data breach r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish automated notification systems for immediate alerts", "2": "Regularly tes
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 785:
RiskId: 2007
ComplianceId: 2667
RiskTitle: Unclear Incident Response Team Responsibility
Criticality: Medium
PossibleDamage: Delays in breach notification and ineffective response
Category: Operational
RiskType: Current
BusinessImpact: Business units with Incident Response Teams
RiskDescription: Lack of clear responsibility within the Incident Response Team may lead to delays in
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 43.2
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clearly define roles and responsibilities within the Incident Response Team", "2":
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 786:
RiskId: 2008
ComplianceId: 2668
RiskTitle: Data Breach Risk from Non-compliant Data Intermediaries
Criticality: High
PossibleDamage: Data breaches, legal penalties, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, loss of customer trust
RiskDescription: Failure to conduct due diligence on data intermediaries may lead to data breaches an

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly audit data intermediary compliance", "2": "Implement data encryption fo
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 787:
RiskId: 2009
ComplianceId: 2669
RiskTitle: Non-Compliance with Data Protection Obligations in Contracts
Criticality: High
PossibleDamage: Unauthorized use or disclosure of personal data, regulatory fines, and reputational d
Category: Legal
RiskType: Current
BusinessImpact: Legal and reputational damage
RiskDescription: Failure to include data protection obligations in contracts may result in data intermedia
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and auditing of contracts", "2": "Training data intermediaries o
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 788:
RiskId: 2010

ComplianceId: 2670
RiskTitle: Inadequate Breach Notification Procedures in Contracts
Criticality: High
PossibleDamage: Delayed or inadequate response to data breaches, regulatory penalties, and reputat
Category: Legal
RiskType: Current
BusinessImpact: Legal and reputational damage
RiskDescription: Lack of clear breach notification procedures in contracts may result in delayed or insu
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 65.7
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on breach response protocols", "2": "Conducting breach respons
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 789:
RiskId: 2011
ComplianceId: 2671
RiskTitle: Failure to Notify Data Breaches
Criticality: High
PossibleDamage: Reputational harm, financial losses, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Significant financial losses, regulatory fines, loss of customer trust
RiskDescription: Failure to notify data breaches in a timely manner can lead to severe consequences f
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement incident response plan", "2": "Regularly test breach notification proced
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 790:
RiskId: 2012
ComplianceId: 2672
RiskTitle: Inadequate Breach Notifications
Criticality: Medium
PossibleDamage: Ineffective response, further data exposure, regulatory penalties
Category: Operational
RiskType: Current
BusinessImpact: Delayed response, increased data exposure, regulatory scrutiny
RiskDescription: Inadequate breach notifications can hinder the organization's ability to respond effecti
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels for breach notifications", "2": "Regularly r
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 791:
RiskId: 2013
ComplianceId: 2673
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data exposure, financial losses, reputational damage

Category: Operational
RiskType: Current
BusinessImpact: Potential loss of customer trust and legal consequences
RiskDescription: Risk of data breach due to inadequate protection provided by data intermediary
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly monitor data intermediary compliance", "2": "Implement data encryption
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 792:
RiskId: 2014
ComplianceId: 2674
RiskTitle: Legal Non-Compliance Risk
Criticality: Medium
PossibleDamage: Regulatory fines, legal penalties
Category: Legal
RiskType: Current
BusinessImpact: Financial losses and reputational damage
RiskDescription: Risk of legal non-compliance due to inadequate documentation and assessment of ov
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Maintain detailed compliance records", "2": "Regularly update compliance assess
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 793:
RiskId: 2015
ComplianceId: 2675
RiskTitle: Ineffective Consent Withdrawal Mechanism
Criticality: High
PossibleDamage: Loss of trust and reputation, potential legal consequences
Category: Compliance
RiskType: Residual
BusinessImpact: Legal actions, reputational damage, loss of customers
RiskDescription: Failure to provide a functional consent withdrawal mechanism may result in individual
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly test the functionality of the withdrawal mechanism", "2": "Provide clear i
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 794:
RiskId: 2016
ComplianceId: 2676
RiskTitle: Ineffective Quarterly Review Process
Criticality: Medium
PossibleDamage: Non-compliance with regulations, inefficient withdrawal process
Category: Compliance
RiskType: Residual
BusinessImpact: Regulatory fines, inefficiencies in withdrawal process
RiskDescription: Failure to conduct quarterly reviews of the withdrawal process may result in outdated

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Document review findings and actions taken", "2": "Implement improvements bas
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 795:
RiskId: 2017
ComplianceId: 2677
RiskTitle: Misunderstanding of Consent Forms
Criticality: High
PossibleDamage: Misunderstanding of consent requirements leading to unauthorized data collection
Category: Compliance
RiskType: Current
BusinessImpact: All departments involved in data collection
RiskDescription: Individuals may provide consent without fully understanding the purposes of data coll
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training to staff on how to explain consent forms clearly", "2": "Regularly r
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 796:
RiskId: 2018

ComplianceId: 2678
RiskTitle: Inadequate Staff Training on Consent Requirements
Criticality: Medium
PossibleDamage: Inadequate training leading to improper collection of consent
Category: Compliance
RiskType: Current
BusinessImpact: All departments involved in data collection
RiskDescription: Staff may provide incorrect information on consent requirements due to inadequate tr
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training sessions on consent requirements", "2": "Provide resources for s
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 797:
RiskId: 2019
ComplianceId: 2679
RiskTitle: Inaccurate Consent Tracking
Criticality: High
PossibleDamage: Unauthorized data processing or non-compliance penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial and reputational damage
RiskDescription: Failure to maintain accurate consent records may result in unauthorized data process
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits of the consent management system", "2": "Implement automated a

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 798:

RiskId: 2020

ComplianceId: 2680

RiskTitle: Outdated Consent Records

Criticality: Medium

PossibleDamage: Non-compliance risks due to outdated or inaccurate records

Category: Operational

RiskType: Inherent

BusinessImpact: Potential legal and reputational consequences

RiskDescription: Failure to conduct annual reviews of consent records may result in outdated or inaccu

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish a clear schedule for annual reviews", "2": "Automate reminders for revie

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 799:

RiskId: 2021

ComplianceId: 2681

RiskTitle: Data Breach due to Lack of Encryption

Criticality: High

PossibleDamage: Financial penalties, reputational damage, legal consequences

Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, legal liabilities
RiskDescription: Unauthorized access to personal data due to lack of encryption controls
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption controls", "2": "Regularly update encryption keys", "3": "Trai
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 800:
RiskId: 2022
ComplianceId: 2682
RiskTitle: Unauthorized Access to Personal Data
Criticality: Medium
PossibleDamage: Data breaches, privacy violations, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Unauthorized individuals gaining access to personal data due to inadequate access c
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement access controls", "2": "Regularly review access permissions", "3": "Co
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 801:
RiskId: 2023
ComplianceId: 2683
RiskTitle: Unauthorized Data Retention
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential financial penalties, loss of customer trust
RiskDescription: Failure to delete personal data after the retention period expires may lead to unautho
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated data deletion processes", "2": "Regularly review and updat
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 802:
RiskId: 2024
ComplianceId: 2684
RiskTitle: Insecure Data Deletion
Criticality: Medium
PossibleDamage: Data leakage, legal liabilities, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential legal actions, loss of customer trust
RiskDescription: Improper deletion of data may leave remnants that can be recovered, leading to unau

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement data encryption before deletion", "2": "Use secure deletion tools to ove
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 803:
RiskId: 2025
ComplianceId: 2685
RiskTitle: Failure to Establish Breach Notification Protocol
Criticality: High
PossibleDamage: Legal consequences, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential legal liabilities and loss of trust from customers and stakeholders.
RiskDescription: Failure to establish a breach notification protocol may result in delayed or inadequate
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on breach notification procedures", "2"
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 804:
RiskId: 2026

ComplianceId: 2686
RiskTitle: Delay in Notification of Data Breaches
Criticality: High
PossibleDamage: Further data exposure, increased impact on affected individuals, regulatory penalties
Category: Operational
RiskType: Current
BusinessImpact: Potential legal liabilities and loss of trust from customers and stakeholders.
RiskDescription: Delay in notifying the affected organization of data breaches may result in further data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish automated notification systems for immediate alerts", "2": "Maintain a de
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 805:
RiskId: 2027
ComplianceId: 2687
RiskTitle: Non-Compliance with Data Processing Agreement
Criticality: High
PossibleDamage: Legal penalties, reputational damage, data breaches
Category: Legal
RiskType: Current
BusinessImpact: Legal consequences and financial losses
RiskDescription: Failure to establish data processing agreements may result in legal penalties, data br
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Legal review of agreements", "2": "Regular compliance audits", "3": "Data protecti
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 806:
RiskId: 2028
ComplianceId: 2688
RiskTitle: Data Encryption Vulnerability
Criticality: High
PossibleDamage: Data breaches and privacy violations
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, legal consequences, damage to reputation
RiskDescription: Failure to encrypt personal data can result in unauthorized access and data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption best practices", "2": "Regularly update encryption keys", "3"
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 807:
RiskId: 2029
ComplianceId: 2689
RiskTitle: Security Assessment Failure
Criticality: Medium
PossibleDamage: Data breaches and non-compliance

Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory fines, reputational damage
RiskDescription: Failure to conduct regular security assessments can result in undetected vulnerabilitie
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement regular security assessment schedules", "2": "Address identified vulne
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 808:
RiskId: 2030
ComplianceId: 2690
RiskTitle: Non-Compliant Handling of Access Requests
Criticality: High
PossibleDamage: Regulatory fines, legal actions, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Delayed or non-compliant responses to access requests, leading to potential financia
RiskDescription: Failure to establish a formal process for handling access requests may result in delay
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for designated staff members on access request handling proced
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 809:
RiskId: 2031
ComplianceId: 2691
RiskTitle: Data Inaccuracy Risk
Criticality: High
PossibleDamage: Inaccurate data leading to faulty decision-making
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to address correction requests may result in incorrect data remaining in the sy
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of correction request handling process", "2": "Training for staff resp
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 810:
RiskId: 2032
ComplianceId: 2692
RiskTitle: Timely Acknowledgment Risk
Criticality: Medium
PossibleDamage: Legal implications and reputational damage
Category: Legal
RiskType: Inherent
BusinessImpact: Potential legal fees and damage to organizational reputation
RiskDescription: Failure to acknowledge correction requests within the specified timeline may result in

RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated acknowledgment system implementation", "2": "Regular training on tim
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 811:
RiskId: 2033
ComplianceId: 2693
RiskTitle: Unauthorized Access to Personal Data
Criticality: High
PossibleDamage: Data breaches, privacy violations, legal consequences
Category: Operational
RiskType: Inherent
BusinessImpact: Potential loss of customer trust, legal penalties, financial losses
RiskDescription: Unauthorized individuals gaining access to personal data can lead to data breaches a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for personnel on verifying identity documents", "2": "Implement m
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 812:
RiskId: 2034

ComplianceId: 2694
RiskTitle: Delays in Verification Process
Criticality: Medium
PossibleDamage: Delays in access requests, potential disputes, and non-compliance with data protect
Category: Operational
RiskType: Inherent
BusinessImpact: Potential delays in providing access to individuals' personal data, disputes, and regula
RiskDescription: Failure to verify identities within the specified timeframe can lead to delays in providin
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear escalation procedures for delayed verification processes", "2": "Re
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 813:
RiskId: 2035
ComplianceId: 2695
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breach, loss of confidentiality
Category: Operational
RiskType: Current
BusinessImpact: Loss of trust, legal implications
RiskDescription: Unauthorized access to sensitive data due to inefficient assessment process
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strict access controls", "2": "Regularly monitor access logs", "3": "Encr

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 814:

RiskId: 2036

ComplianceId: 2696

RiskTitle: Data Disclosure Risk

Criticality: Medium

PossibleDamage: Legal penalties, loss of trust

Category: Legal

RiskType: Current

BusinessImpact: Legal disputes, reputational damage

RiskDescription: Disclosure of data without proper consent leading to legal consequences

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement consent management system", "2": "Train staff on consent procedures

CreatedAt: 2025-10-30 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 815:

RiskId: 2037

ComplianceId: 2697

RiskTitle: Non-Compliance with Data Consent Requirements

Criticality: High

PossibleDamage: Legal penalties, reputational damage

Category: Compliance
RiskType: Inherent
BusinessImpact: Potential legal fines, loss of trust from employees
RiskDescription: Failure to obtain proper consent for employee data handling may lead to legal conseq
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust consent management processes", "2": "Regularly review and up
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 816:
RiskId: 2038
ComplianceId: 2698
RiskTitle: Data Access Request Mishandling
Criticality: Medium
PossibleDamage: Data breaches, legal consequences
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential data leaks, legal penalties
RiskDescription: Improper handling of data access requests may lead to unauthorized data disclosures
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement access control measures", "2": "Train staff on data access procedures
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 817:
RiskId: 2039
ComplianceId: 2699
RiskTitle: Misunderstanding of Data Usage
Criticality: High
PossibleDamage: Loss of trust and credibility
Category: Compliance
RiskType: Inherent
BusinessImpact: Loss of customer trust and potential legal consequences
RiskDescription: Individuals may feel misled or deceived about how their data is being used, leading to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide clear examples of data usage purposes", "2": "Offer easy access to conta
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 818:
RiskId: 2040
ComplianceId: 2700
RiskTitle: Inconsistent Communication
Criticality: Medium
PossibleDamage: Confusion and lack of trust
Category: Compliance
RiskType: Inherent
BusinessImpact: Internal departments may face challenges in data handling and compliance
RiskDescription: Inconsistencies in communication of data purposes may lead to confusion among indi

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide training on template usage", "2": "Regularly audit template adherence", "3
CreatedAt: 2025-10-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 819:
RiskId: 1763
ComplianceId: 2417
RiskTitle: Lack of Oversight by Senior Information Security Official
Criticality: High
PossibleDamage: Increased risk of data breaches and non-compliance due to lack of oversight
Category: Operational
RiskType: Inherent
BusinessImpact: All business units within the organization
RiskDescription: Failure to appoint a senior information security official may result in inadequate oversi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely appointment of a qualified official", "2": "Provide necessary resourc
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 820:
RiskId: 1764

ComplianceId: 2418
RiskTitle: Inadequate Resource Allocation for Security Initiatives
Criticality: Medium
PossibleDamage: Increased vulnerability to cyber threats and non-compliance due to lack of resources
Category: Operational
RiskType: Inherent
BusinessImpact: All business units within the organization
RiskDescription: Insufficient resource allocation for security initiatives may result in gaps in protection,
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly assess resource needs for security initiatives", "2": "Allocate budget and
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 821:
RiskId: 1765
ComplianceId: 2419
RiskTitle: Security Breach Due to Lack of Awareness
Criticality: High
PossibleDamage: Potential data loss, reputational damage, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Significant disruption to operations, loss of customer trust
RiskDescription: Failure to comply with security awareness training may lead to employees and third p
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular security audits and assessments", "2": "Continuous monitoring of access
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 822:
RiskId: 1766
ComplianceId: 2420
RiskTitle: Ineffective Security Management Forum
Criticality: High
PossibleDamage: Increased vulnerabilities and potential security breaches
Category: Operational
RiskType: Current
BusinessImpact: Disruption to business operations, financial losses, reputational damage
RiskDescription: Lack of coordination and alignment on security initiatives leading to increased vulnera
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear agenda and objectives for each forum meeting", "2": "Ensure activ
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 823:
RiskId: 1767
ComplianceId: 2421
RiskTitle: Data Breach Risk Due to Ineffective Security Program Assessment
Criticality: High
PossibleDamage: Loss of sensitive information, financial losses, reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: All business units would suffer financial and reputational damage
RiskDescription: Failure to conduct an annual security program assessment by an independent third-pa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Engage reputable third-party assessors", "2": "Implement recommendations from
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 824:
RiskId: 1768
ComplianceId: 2422
RiskTitle: Lack of Oversight by CISO
Criticality: High
PossibleDamage: Security incidents not being promptly addressed or communicated
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to designate a CISO may result in security incidents not being promptly addres
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure CISO is well-trained and qualified", "2": "Implement backup CISO plan", "3
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 825:
RiskId: 1769
ComplianceId: 2423
RiskTitle: Lack of Regular Security Policy Review
Criticality: Medium
PossibleDamage: Non-compliance and security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to conduct quarterly security meetings may result in security policies not being
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear meeting agendas and objectives", "2": "Ensure participation of key
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 826:
RiskId: 1770
ComplianceId: 2424
RiskTitle: Increased Vulnerability to Security Threats
Criticality: High
PossibleDamage: Potential data breaches, loss of sensitive information, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units within the organization may be impacted by security incidents resul
RiskDescription: Failure to complete mandatory information security training may lead to gaps in knowl

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reminders and notifications to employees about upcoming training deadli
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 827:
RiskId: 1771
ComplianceId: 2425
RiskTitle: Ineffective Response to Security Threats
Criticality: Medium
PossibleDamage: Increased risk of falling victim to social engineering attacks, data breaches, and mal
Category: Operational
RiskType: Residual
BusinessImpact: All business units within the organization may be impacted by security incidents resul
RiskDescription: Failure to assess and improve employee awareness levels through surveys and exer
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update and customize phishing exercises to reflect current threats and
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 828:
RiskId: 1772

ComplianceId: 2426
RiskTitle: Confusion and Lack of Accountability in Information Security Roles
Criticality: High
PossibleDamage: Increased security risks, data breaches, and compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Potential disruption of operations and loss of sensitive information
RiskDescription: Failure to identify and document information security roles may lead to confusion, lack
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure all roles are correctly identified and documented", "2": "T
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 829:
RiskId: 1773
ComplianceId: 2427
RiskTitle: Outdated Information Security Roles
Criticality: Medium
PossibleDamage: Misalignment with security needs, increased vulnerabilities
Category: Operational
RiskType: Residual
BusinessImpact: Potential security gaps and inefficiencies in security management
RiskDescription: Failure to review information security roles may result in outdated assignments, misal
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish a formal review process with defined timelines and responsibilities", "2":

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 830:

RiskId: 1774

ComplianceId: 2428

RiskTitle: Security Responsibilities Review Failure

Criticality: High

PossibleDamage: Unauthorized access to sensitive information, data breaches, and reputational dama

Category: Operational

RiskType: Residual

BusinessImpact: All business units would be impacted by potential security breaches

RiskDescription: Failure to review and update security responsibilities may lead to ineffective manage

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Schedule regular annual reviews of security responsibilities", "2": "Implement a cl

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 831:

RiskId: 1775

ComplianceId: 2429

RiskTitle: Confusion in Security Roles and Responsibilities

Criticality: High

PossibleDamage: Confusion may lead to unauthorized access and security breaches

Category: Operational
RiskType: Current
BusinessImpact: Potential security breaches impacting all business units
RiskDescription: Lack of clear documentation and understanding of security roles may result in unauth
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on security roles and responsibilities", "2": "Automated
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 832:
RiskId: 1776
ComplianceId: 2430
RiskTitle: Phishing Attacks Targeting New Employees
Criticality: High
PossibleDamage: Loss of sensitive information, financial loss
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, reputational damage
RiskDescription: New employees may unknowingly fall victim to phishing attacks, leading to potential d
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update employees on latest phishing tactics", "2": "Implement multi-fact
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 833:
RiskId: 1777
ComplianceId: 2431
RiskTitle: Social Engineering Attacks Due to Lack of Awareness
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal consequences
RiskDescription: Employees may unknowingly disclose sensitive information or fall for social engineeri
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide ongoing phishing awareness training", "2": "Implement strict access contr
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 834:
RiskId: 1778
ComplianceId: 2432
RiskTitle: Data Breach Due to Unauthorized Information Asset Access
Criticality: High
PossibleDamage: Loss of sensitive information, reputational damage, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial losses, legal consequences
RiskDescription: Unauthorized access to new information assets could result in a data breach, leading

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and user authentication mechanisms", "2": "Regu
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 835:
RiskId: 1779
ComplianceId: 2433
RiskTitle: Data Breach Due to Outdated Security Measures
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal consequences
Category: Compliance
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to conduct annual reviews may result in security vulnerabilities that could be e
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular security training for employees", "2": "Utilize automated monito
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 836:
RiskId: 1780

ComplianceId: 2434
RiskTitle: Breach of Confidentiality
Criticality: High
PossibleDamage: Legal consequences due to unauthorized disclosure
Category: Compliance
RiskType: Current
BusinessImpact: Legal actions, financial penalties
RiskDescription: Failure to comply with confidentiality agreements may result in legal actions and finan
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on confidentiality policies", "2": "Implement encryption measures
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 837:
RiskId: 1781
ComplianceId: 2435
RiskTitle: Non-Compliance with Legislative Changes
Criticality: Medium
PossibleDamage: Legal risks due to outdated agreements
Category: Legal
RiskType: Current
BusinessImpact: Legal actions, fines
RiskDescription: Failure to update agreements in line with new legislation may expose the organizatior
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regular monitoring of legislative changes", "2": "Engage legal counsel for review

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 838:

RiskId: 1782

ComplianceId: 2436

RiskTitle: Unauthorized Disclosure Risk

Criticality: High

PossibleDamage: Unauthorized disclosure of confidential information

Category: Compliance

RiskType: Residual

BusinessImpact: Legal consequences, loss of trust, financial penalties.

RiskDescription: The risk of unauthorized personnel signing confidentiality agreements leading to brea

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training sessions on authorized signatories", "2": "Automated alerts for ur

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 839:

RiskId: 1783

ComplianceId: 2437

RiskTitle: Failure to Document Incident Reporting Procedures

Criticality: High

PossibleDamage: Delayed or inaccurate reporting of security incidents, potential legal and regulatory c

Category: Operational
RiskType: Current
BusinessImpact: All business units within the organization may be affected by delayed or inaccurate in
RiskDescription: Failure to document incident reporting procedures may lead to confusion, delays, and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure documentation accuracy", "2": "Training sessions on inc
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 840:
RiskId: 1784
ComplianceId: 2438
RiskTitle: Lack of Incident Reporting Procedures Training
Criticality: Medium
PossibleDamage: Mishandling of security incidents, increased risks, potential legal consequences
Category: Operational
RiskType: Current
BusinessImpact: All business units within the organization may be affected by mishandling of security i
RiskDescription: Lack of training on incident reporting procedures may lead to errors, mishandling, and
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training sessions on incident reporting procedures", "2": "Testing and cer
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 841:
RiskId: 1785
ComplianceId: 2439
RiskTitle: Lack of Annual Review of Roles and Responsibilities
Criticality: High
PossibleDamage: Failure to review roles and responsibilities may lead to mismanagement of informati
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential data breaches and non-compliance
RiskDescription: Failure to conduct annual reviews of roles and responsibilities could result in employe
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide regular training and awareness sessions on information security practices
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 842:
RiskId: 1786
ComplianceId: 2440
RiskTitle: Delay in Updating Roles and Responsibilities
Criticality: Medium
PossibleDamage: Delay in updating roles and responsibilities may lead to miscommunication, confusio
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential security incidents and non-compliar
RiskDescription: Failure to update roles and responsibilities immediately when there are changes coul

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a clear process for notifying relevant personnel of changes in roles and
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 843:
RiskId: 1787
ComplianceId: 2441
RiskTitle: Outdated Security Practices
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats
Category: Operational
RiskType: Residual
BusinessImpact: Information Security Department
RiskDescription: Lack of engagement with special interest groups may result in outdated security pract
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update membership list", "2": "Encourage participation in gr
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 844:
RiskId: 1788

ComplianceId: 2442
RiskTitle: Missed Opportunities for Collaboration
Criticality: Medium
PossibleDamage: Missed opportunities for knowledge sharing and collaboration
Category: Operational
RiskType: Residual
BusinessImpact: Information Security Department
RiskDescription: Lack of tracking participation in special interest group activities may result in missed c
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a tracking system for participation", "2": "Regularly review participation
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 845:
RiskId: 1789
ComplianceId: 2443
RiskTitle: Appointment of Unqualified Reviewers
Criticality: High
PossibleDamage: Inaccurate or incomplete review findings, leading to unidentified security vulnerabiliti
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may be affected by security vulnerabilities
RiskDescription: Failure to appoint qualified reviewers may result in inadequate review outcomes, leav
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Ensure thorough vetting process for selecting reviewers", "2": "Provide training to

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 846:

RiskId: 1790

ComplianceId: 2444

RiskTitle: Lack of Annual Reviews

Criticality: Medium

PossibleDamage: Outdated security measures and ineffective risk management

Category: Operational

RiskType: Inherent

BusinessImpact: All business units may be affected by outdated security measures

RiskDescription: Failure to conduct annual reviews may result in the organization being unaware of ne

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish a review schedule and adhere to it consistently", "2": "Implement autom

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 847:

RiskId: 1791

ComplianceId: 2445

RiskTitle: Failure to Document Independent Review Findings

Criticality: High

PossibleDamage: Security breaches due to unidentified risks

Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, reputational damage, and legal consequences
RiskDescription: Failure to document findings may result in critical security vulnerabilities not being add
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation procedures", "2": "Automated documentation t
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 848:
RiskId: 1792
ComplianceId: 2446
RiskTitle: Failure to Conduct Annual Risk Assessment
Criticality: High
PossibleDamage: Increased exposure to security threats and vulnerabilities
Category: IT
RiskType: Residual
BusinessImpact: All business units may face disruptions and financial losses
RiskDescription: Failure to conduct annual risk assessments may lead to unidentified vulnerabilities an
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely risk assessments are conducted", "2": "Implement automated risk a
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 849:
RiskId: 1793
ComplianceId: 2447
RiskTitle: Delay in Conducting Risk Assessment after Significant Changes
Criticality: Medium
PossibleDamage: Increased exposure to threats and vulnerabilities
Category: IT
RiskType: Residual
BusinessImpact: All business units may face disruptions and compliance issues
RiskDescription: Delay in conducting risk assessments after significant changes may lead to unaddres
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear criteria for identifying significant changes", "2": "Implement automa
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 850:
RiskId: 1794
ComplianceId: 2448
RiskTitle: Vendor Security Vulnerabilities
Criticality: High
PossibleDamage: Data breaches, unauthorized access
Category: IT
RiskType: Inherent
BusinessImpact: Loss of sensitive data, reputational damage
RiskDescription: Failure to assess vendor security risks may lead to data breaches and unauthorized a

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Thorough vendor assessments", "2": "Implement security controls", "3": "Regular
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 851:
RiskId: 1795
ComplianceId: 2449
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of customer trust
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of unauthorized access to sensitive customer data due to inadequate security me
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls and authentication mechanisms", "2": "Regular
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 852:
RiskId: 1796

ComplianceId: 2450
RiskTitle: Outdated Security Measures Risk
Criticality: Medium
PossibleDamage: Increased vulnerability to cyber threats, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of outdated security measures leading to vulnerabilities and potential data breac
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update security requirements based on industry best practices", "2": "C
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 853:
RiskId: 1797
ComplianceId: 2451
RiskTitle: Data Breach Due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive customer information, financial penalties, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: IT Security, Legal, Compliance
RiskDescription: Unauthorized access to sensitive information leading to a data breach, financial penal
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and regular access reviews", "2": "Encrypt sensit
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 854:
RiskId: 1798
ComplianceId: 2452
RiskTitle: Data Leak Due to Unnecessary Access
Criticality: Medium
PossibleDamage: Loss of sensitive information, reputational damage, compliance fines
Category: Operational
RiskType: Current
BusinessImpact: IT Security, Legal, Compliance
RiskDescription: Data leak due to unnecessary access to sensitive information, leading to reputational
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update access permissions", "2": "Implement data loss prev
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 855:
RiskId: 1799
ComplianceId: 2453
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access leading to data breaches or misuse of sensitive information

Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of unauthorized users gaining access to sensitive information, leading to potentia
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for access control", "2": "Regularly review a
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 856:
RiskId: 1800
ComplianceId: 2454
RiskTitle: Access Request Approval Risk
Criticality: Medium
PossibleDamage: Unauthorized access due to lack of review and approval processes
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of unauthorized access due to inadequate review and approval processes, leadi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 43.2
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated access review processes", "2": "Enforce strict access appro
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 857:
RiskId: 1801
ComplianceId: 2455
RiskTitle: Delayed Incident Reporting
Criticality: High
PossibleDamage: Increased exposure to security threats and potential data breaches
Category: Operational
RiskType: Current
BusinessImpact: Potential compromise of sensitive information and disruption of business operations
RiskDescription: Failure to report incidents immediately may lead to prolonged exposure to security ris
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular incident reporting training for all employees", "2": "Automate in
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 858:
RiskId: 1802
ComplianceId: 2456
RiskTitle: Delayed Incident Investigations
Criticality: Medium
PossibleDamage: Prolonged exposure to security threats and incomplete incident resolution
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of repeated incidents, regulatory non-compliance, and compromised se
RiskDescription: Delays in initiating incident investigations may lead to incomplete incident resolution, i

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear investigation procedures and timelines", "2": "Implement automate
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 859:
RiskId: 1803
ComplianceId: 2457
RiskTitle: Data Breach Due to Inadequate Third-Party Security Controls
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage, legal implications.
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, loss of customer trust.
RiskDescription: Inadequate security controls in third-party agreements may lead to unauthorized acce
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security audits of third-party systems", "2": "Enforce strong data encryptio
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 860:
RiskId: 1804

ComplianceId: 2458
RiskTitle: Legal Non-Compliance Due to Unapproved Third-Party Agreements
Criticality: Medium
PossibleDamage: Contractual disputes, legal penalties, reputational damage.
Category: Legal
RiskType: Current
BusinessImpact: Legal repercussions, financial losses, damage to organizational reputation.
RiskDescription: Failure to obtain legal and compliance team approval for third-party agreements may
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear approval workflows for third-party agreements", "2": "Provide legal
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 861:
RiskId: 1805
ComplianceId: 2459
RiskTitle: Failure to Include Security Controls in Third-Party Agreements
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: All business units relying on third-party services
RiskDescription: Failure to include security controls in third-party agreements may lead to unauthorized
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular monitoring of third-party compliance with security controls", "2": "Impleme

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 862:

RiskId: 1806

ComplianceId: 2460

RiskTitle: Lack of Incident Reporting Procedures in Third-Party Agreements

Criticality: Medium

PossibleDamage: Delayed detection and response to security incidents, extended downtime, data loss

Category: Operational

RiskType: Residual

BusinessImpact: All business units relying on third-party services

RiskDescription: Failure to include incident reporting procedures in third-party agreements may lead to

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establishing clear incident reporting requirements in agreements", "2": "Conductin

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 863:

RiskId: 1807

ComplianceId: 2461

RiskTitle: Delayed Incident Notification

Criticality: High

PossibleDamage: Increased data breach impact, regulatory fines, reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, damage to reputation, legal consequences
RiskDescription: Failure to notify the organization within the specified timeline may result in prolonged
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish automated incident reporting mechanisms", "2": "Regularly review vend
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 864:
RiskId: 1808
ComplianceId: 2462
RiskTitle: Insecure Communication Channels
Criticality: Medium
PossibleDamage: Data leakage, unauthorized access, compromised incident response
Category: IT
RiskType: Inherent
BusinessImpact: Potential data breaches, loss of sensitive information, regulatory non-compliance
RiskDescription: Failure to use secure communication channels for incident reporting may expose sens
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement end-to-end encryption for incident reporting channels", "2": "Regularly
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 865:
RiskId: 1809
ComplianceId: 2463
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Unauthorized access to sensitive information can lead to data breaches and compron
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for sensitive data access", "2": "Regularly m
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 866:
RiskId: 1810
ComplianceId: 2464
RiskTitle: Documentation Gap Risk
Criticality: Medium
PossibleDamage: Confusion or unauthorized access
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Lack of documentation for access privilege changes can lead to confusion among per

RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated access change tracking tools", "2": "Enforce strict documer
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 867:
RiskId: 1811
ComplianceId: 2465
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, reputational damage, financial losses.
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of third-party vendors gaining unauthorized access to sensitive information and c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review of access agreements", "2": "Training for Procurement Departmer
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 868:
RiskId: 1812

ComplianceId: 2466
RiskTitle: Outdated Access Permissions Risk
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches, compliance violations.
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of outdated access permissions leading to unauthorized access, potential data b
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated access review processes", "2": "Regular training for employees on acc
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 869:
RiskId: 1813
ComplianceId: 2467
RiskTitle: Failure to Acknowledge Data Subject Rights Requests
Criticality: High
PossibleDamage: Legal penalties, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Delayed response to data subject rights requests, legal consequences
RiskDescription: Failure to acknowledge data subject rights requests within the specified timeline may
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement automated acknowledgment system", "2": "Regular training for staff on

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 870:

RiskId: 1814

ComplianceId: 2468

RiskTitle: Failure to Fulfill Data Subject Rights Requests

Criticality: High

PossibleDamage: Legal consequences, reputational harm

Category: Compliance

RiskType: Residual

BusinessImpact: Legal penalties, reputational damage

RiskDescription: Failure to fulfill data subject rights requests within the specified timeline may lead to le

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear process for request fulfillment", "2": "Regular monitoring of reques

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 871:

RiskId: 1815

ComplianceId: 2469

RiskTitle: Unauthorized Processor Engagement

Criticality: High

PossibleDamage: Data breaches and regulatory fines

Category: Compliance
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Engaging processors without proper authorization can lead to unauthorized processin
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a formal authorization process for engaging processors", "2": "Regular
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 872:
RiskId: 1816
ComplianceId: 2470
RiskTitle: Non-Compliant Processor Engagement
Criticality: Medium
PossibleDamage: Regulatory fines and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Engaging processors that are not compliant with GDPR requirements can lead to regu
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update the registry with compliance status of processors", "2": "Conduc
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 873:
RiskId: 1817
ComplianceId: 2471
RiskTitle: Risk of Hiring Individuals with Criminal Records
Criticality: High
PossibleDamage: Security breaches, legal liabilities, damage to reputation
Category: Operational
RiskType: Current
BusinessImpact: Potential legal actions, financial losses, reputational damage
RiskDescription: Hiring individuals with criminal records poses a significant risk to the organization's se
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify criminal background through reputable third-party services", "2": "Review re
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 874:
RiskId: 1818
ComplianceId: 2472
RiskTitle: Risk of Falsified Employment History
Criticality: Medium
PossibleDamage: Incompetence in roles, decreased productivity, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of productivity, potential legal issues, damage to reputation
RiskDescription: Hiring individuals based on falsified employment history poses a risk of incompetence

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Contact previous employers directly for verification", "2": "Cross-check information
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 875:
RiskId: 1819
ComplianceId: 2473
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches and compromised security
RiskDescription: Risk of unauthorized individuals gaining access to sensitive information due to undefi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and authentication measures", "2": "Regularly re
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 876:
RiskId: 1820

ComplianceId: 2474
RiskTitle: Failure to Initiate Background Verification Checks
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, potential security breaches, legal impl
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of sensitive data, damage to reputation, legal penalties
RiskDescription: Failure to initiate background verification checks can lead to unauthorized access to s
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access control measures", "2": "Regularly review and update bac
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 877:
RiskId: 1821
ComplianceId: 2475
RiskTitle: Incomplete or Delayed Background Verification Checks
Criticality: Medium
PossibleDamage: Incomplete or delayed verification checks, increased risk of hiring individuals with qu
Category: Operational
RiskType: Inherent
BusinessImpact: Increased risk of security breaches, legal consequences, damage to reputation
RiskDescription: Incomplete or delayed background verification checks can lead to hiring individuals w
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement automated reminders for pending checks", "2": "Establish clear escala

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 878:

RiskId: 1822

ComplianceId: 2476

RiskTitle: Unauthorized Access to Sensitive Information

Criticality: High

PossibleDamage: Data breaches, compliance violations, reputational damage

Category: Operational

RiskType: Current

BusinessImpact: Potential loss of sensitive data, legal consequences, damage to reputation

RiskDescription: Unauthorized individuals gaining access to sensitive information can lead to data brea

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strict access controls and monitoring mechanisms", "2": "Regularly au

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 879:

RiskId: 1823

ComplianceId: 2477

RiskTitle: Delayed Access Request Reviews

Criticality: Medium

PossibleDamage: Operational inefficiencies, security vulnerabilities

Category: Operational
RiskType: Current
BusinessImpact: Operational delays, potential security risks
RiskDescription: Delays in reviewing access requests can lead to operational inefficiencies and potenti
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear SLAs for access request reviews", "2": "Automate access request
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 880:
RiskId: 1824
ComplianceId: 2478
RiskTitle: Unauthorized Access Risk for New Hires
Criticality: High
PossibleDamage: Unauthorized access to sensitive information leading to data breaches, financial loss
Category: Operational
RiskType: Current
BusinessImpact: Potential financial loss, reputational damage, legal consequences
RiskDescription: Risk of new hires gaining unauthorized access to sensitive information due to insuffici
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and monitoring systems", "2": "Provide regular se
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 881:
RiskId: 1825
ComplianceId: 2479
RiskTitle: Reinvestigation Gap Risk
Criticality: Medium
PossibleDamage: Failure to detect changes in personnel background leading to increased risk of inside
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of insider threats, unauthorized access to sensitive information
RiskDescription: Risk of not conducting timely reinvestigations leading to undetected changes in perso
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate reinvestigation process to ensure timely checks", "2": "Implement contin
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 882:
RiskId: 1826
ComplianceId: 2480
RiskTitle: Data Breach due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive information, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, legal consequences, loss of customer trust
RiskDescription: Unauthorized access to sensitive information can lead to data breaches and significan

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security audits and monitoring", "2": "Encryption of sensitive data", "3": "I
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 883:
RiskId: 1827
ComplianceId: 2481
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, legal consequences
RiskDescription: Unauthorized access to sensitive information due to lack of signed agreements.
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on access agreement policies", "2": "Automated reminders for ag
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 884:
RiskId: 1828

ComplianceId: 2482
RiskTitle: Outdated Agreement Risk
Criticality: Medium
PossibleDamage: Unauthorized access, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions, legal consequences
RiskDescription: Outdated access agreements not reflecting current access requirements.
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated reminders for annual reviews", "2": "Regular training on agreement rev
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 885:
RiskId: 1829
ComplianceId: 2483
RiskTitle: Non-Completion of Security Awareness Training
Criticality: High
PossibleDamage: Increased vulnerability to security threats, potential data breaches, and non-complia
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to complete security awareness training exposes the organization to higher ris
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular reminders and notifications for training deadlines", "2": "Provide incentive

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 886:

RiskId: 1830

ComplianceId: 2484

RiskTitle: Lack of Essential Training Content Awareness

Criticality: High

PossibleDamage: Increased risk of data breaches, non-compliance, and security incidents

Category: Operational

RiskType: Residual

BusinessImpact: Potential financial losses, reputational damage, and legal consequences

RiskDescription: Employees may not be adequately trained on essential security procedures, increasin

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly review and update training content to ensure it remains relevant and co

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 887:

RiskId: 1831

ComplianceId: 2485

RiskTitle: Infrequent Security Training Updates

Criticality: Medium

PossibleDamage: Increased risk of security incidents due to outdated knowledge and lack of awarenes

Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, reputational damage, and operational disruptions
RiskDescription: Employees may not receive regular updates on security practices, leading to a lack of
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Schedule regular training sessions well in advance to ensure all employees can p
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 888:
RiskId: 1832
ComplianceId: 2486
RiskTitle: Inadequate Security Training for IT Personnel
Criticality: High
PossibleDamage: Data breaches, unauthorized access, compromised security measures
Category: IT
RiskType: Current
BusinessImpact: IT Security Department
RiskDescription: Failure to provide specialized training may result in IT personnel lacking the necessar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update training materials to align with current security threat
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 889:
RiskId: 1833
ComplianceId: 2487
RiskTitle: Outdated Security Training Materials
Criticality: Medium
PossibleDamage: Increased risk of security incidents, gaps in knowledge and skills
Category: IT
RiskType: Current
BusinessImpact: IT Security Department
RiskDescription: Failure to update security training materials may result in personnel being unaware of
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a process for promptly identifying and implementing updates to training
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 890:
RiskId: 1834
ComplianceId: 2488
RiskTitle: Security Breach Due to Untrained New Hires
Criticality: High
PossibleDamage: Financial loss, reputational damage, and legal consequences due to a security brea
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of sensitive data, regulatory fines.
RiskDescription: Failure to train new hires on security awareness could result in them inadvertently cau

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement mandatory training completion deadlines", "2": "Provide clear guideline
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 891:
RiskId: 1835
ComplianceId: 2489
RiskTitle: Phishing Attack Due to Lack of Annual Training
Criticality: Medium
PossibleDamage: Loss of sensitive data, financial loss, and reputational damage due to a successful p
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust, regulatory fines.
RiskDescription: Failure to provide annual security awareness training could result in employees falling
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update training content with examples of current threats", "2": "Simulate
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 892:
RiskId: 1836

ComplianceId: 2490
RiskTitle: Inadequate Incident Response Training
Criticality: High
PossibleDamage: Ineffective response to security incidents, leading to data breaches or system compr
Category: Operational
RiskType: Current
BusinessImpact: Disruption of IT operations, compromise of sensitive data
RiskDescription: Failure to complete incident response training may result in personnel lacking necess
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training completion status", "2": "Provide additional training
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 893:
RiskId: 1837
ComplianceId: 2491
RiskTitle: Incomplete Security Awareness Training Content
Criticality: High
PossibleDamage: Increased risk of data breaches and non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to cover essential topics in training could result in employees lacking crucial kn
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training content", "2": "Feedback mechanisms for content ir
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 894:
RiskId: 1838
ComplianceId: 2492
RiskTitle: Delayed Security Awareness Training
Criticality: Medium
PossibleDamage: Lack of updated knowledge on security practices and policies
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Delaying or missing training sessions could result in employees not being up-to-date
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated reminders for training deadlines", "2": "Tracking and reporting on train
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 895:
RiskId: 1839
ComplianceId: 2493
RiskTitle: Ineffective Incident Response
Criticality: High
PossibleDamage: Extended downtime, data breaches, financial losses

Category: Operational
RiskType: Residual
BusinessImpact: Significant impact on operations, financial stability, and data security
RiskDescription: Failure to respond effectively to security incidents due to lack of training and prepared
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions", "2": "Performance evaluations", "3": "Continuous feedb
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 896:
RiskId: 1840
ComplianceId: 2494
RiskTitle: Inadequate Documentation of Security Violations
Criticality: High
PossibleDamage: Inconsistent disciplinary actions and legal challenges
Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal repercussions and compromised security measures
RiskDescription: Failure to document security violations may lead to inconsistent disciplinary actions, le
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a standardized documentation template", "2": "Provide training on prop
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 897:
RiskId: 1841
ComplianceId: 2495
RiskTitle: Delay in Initiating Disciplinary Process
Criticality: Medium
PossibleDamage: Continued security risks and escalation of violations
Category: Compliance
RiskType: Residual
BusinessImpact: Increased security vulnerabilities and potential breaches
RiskDescription: Delay in initiating the disciplinary process for security violations may lead to continued
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish automated alerts for violation identification", "2": "Define clear escalation
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 898:
RiskId: 1842
ComplianceId: 2496
RiskTitle: Data Breach Due to Delayed Access Revocation
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal consequences.
Category: IT
RiskType: Current
BusinessImpact: Potential loss of sensitive data, financial losses due to legal fines and penalties.
RiskDescription: Failure to immediately revoke access rights upon termination may lead to unauthorize

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated access revocation processes", "2": "Regularly review and u
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 899:
RiskId: 1843
ComplianceId: 2497
RiskTitle: Delayed Asset Recovery
Criticality: Medium
PossibleDamage: Financial losses, misuse of assets, operational disruptions.
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses due to asset misuse or theft, operational disruptions due to
RiskDescription: Failure to recover organizational assets within 48 hours may lead to financial losses, a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement asset tracking systems", "2": "Establish clear asset recovery procedure
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 900:
RiskId: 1844

ComplianceId: 2498
RiskTitle: Risk of Hiring Unvetted Employees
Criticality: High
PossibleDamage: Potential security breaches, data leaks, or reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: All business units could suffer financial losses, legal consequences, and damage to r
RiskDescription: Failure to conduct thorough background checks may result in hiring individuals with m
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust background check process", "2": "Provide ongoing training to
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 901:
RiskId: 1845
ComplianceId: 2499
RiskTitle: Risk of Inadequate Security Awareness Training
Criticality: Medium
PossibleDamage: Security incidents, data breaches, or non-compliance due to lack of employee aware
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face financial losses, reputational damage, and legal repercus
RiskDescription: Insufficient security awareness training for new employees may result in unintentional
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Develop comprehensive security training programs tailored to different job roles",
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 902:
RiskId: 1846
ComplianceId: 2500
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Loss of sensitive information, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of unauthorized access to sensitive information and organizational assets during
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access revocation reviews", "2": "Implement two-factor authentication for
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 903:
RiskId: 1847
ComplianceId: 2501
RiskTitle: Task Completion Delay Risk
Criticality: Medium
PossibleDamage: Incomplete retrieval of organizational assets, delays in termination procedures

Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of delays in completion of termination tasks and retrieval of organizational assets
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular system monitoring for delays", "2": "Implement escalation procedures for
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 904:
RiskId: 1848
ComplianceId: 2502
RiskTitle: Data Breach Due to Unauthorized Access
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Unauthorized access to sensitive information can lead to data breaches, financial loss
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access rights audits", "2": "Training on access rights management", "3": "
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 905:
RiskId: 1849
ComplianceId: 2503
RiskTitle: Delayed Access Removal
Criticality: Medium
PossibleDamage: Unauthorized access, compliance violations, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: HR and IT departments
RiskDescription: Delayed access removal can result in unauthorized access to systems and informatio
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels between HR and IT departments", "2": "F
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 906:
RiskId: 1850
ComplianceId: 2504
RiskTitle: Loss of Organizational Assets
Criticality: High
PossibleDamage: Financial loss, reputational damage, security breaches
Category: Operational
RiskType: Current
BusinessImpact: Loss of critical equipment, compromised data security
RiskDescription: Failure to return organizational assets could result in financial losses, data breaches,

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of asset returns", "2": "Strict enforcement of return procedures", "3
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 907:
RiskId: 1851
ComplianceId: 2505
RiskTitle: Disputes Over Returned Assets
Criticality: Medium
PossibleDamage: Loss of assets, legal disputes, damaged employee relations
Category: Operational
RiskType: Current
BusinessImpact: Disputes could lead to loss of critical assets, legal costs, and strained employee relati
RiskDescription: Failure to provide a receipt for returned assets could result in disputes, legal issues, a
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated asset tracking system", "2": "Employee acknowledgment of receipt", "3
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 908:
RiskId: 1852

ComplianceId: 2506
RiskTitle: Risk of Hiring Individuals with Undisclosed Criminal History
Criticality: High
PossibleDamage: Security breaches, legal liabilities, damage to reputation
Category: Operational
RiskType: Residual
BusinessImpact: Potential security threats, legal consequences, reputational damage
RiskDescription: Failure to conduct criminal history background checks could result in hiring individuals
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a strict background check process", "2": "Review results with HR and s
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 909:
RiskId: 1853
ComplianceId: 2507
RiskTitle: Risk of Hiring Individuals with Falsified Employment or Education History
Criticality: Medium
PossibleDamage: Incompetence, dishonesty, damage to reputation
Category: Operational
RiskType: Residual
BusinessImpact: Potential incompetence, dishonesty, and reputational damage in the workplace
RiskDescription: Failure to verify employment and education history could result in hiring individuals wi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Verify information with previous employers and educational institutions", "2": "Cro

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 910:

RiskId: 1854

ComplianceId: 2508

RiskTitle: Non-Completion of Security Awareness Training

Criticality: High

PossibleDamage: Increased risk of data breaches, unauthorized access, and compromised information

Category: Operational

RiskType: Residual

BusinessImpact: All business units could face financial losses, reputational damage, and legal consequ

RiskDescription: Failure to complete security awareness training increases the likelihood of employees

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enforce strict consequences for non-compliance", "2": "Provide ongoing support a

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 911:

RiskId: 1855

ComplianceId: 2509

RiskTitle: Data Breach Risk

Criticality: High

PossibleDamage: Unauthorized access to sensitive information leading to data breaches

Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Unauthorized access to sensitive data can lead to financial losses, reputational dama
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews to identify and remove any unauthorized access", "2": "Im
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 912:
RiskId: 1856
ComplianceId: 2510
RiskTitle: Inconsistencies in Access Revocation
Criticality: Medium
PossibleDamage: Inconsistencies in access revocation leading to security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Inadequate documentation and inconsistent application of access revocation procedu
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular audits of access revocation procedures to ensure compliance", "2": "Prov
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 913:
RiskId: 1857
ComplianceId: 2511
RiskTitle: Inadequate Information Security Policies
Criticality: High
PossibleDamage: Increased risk of data breaches, regulatory fines, and reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to develop and approve information security policies may expose the organiza
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on policy development and approval pr
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 914:
RiskId: 1858
ComplianceId: 2512
RiskTitle: Security Breach Due to Lack of New Hire Training
Criticality: High
PossibleDamage: Potential data breaches, financial losses, and reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to provide training to new hires may lead to gaps in understanding information

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update training materials", "2": "Provide refresher courses annually", "3"
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 915:
RiskId: 1859
ComplianceId: 2513
RiskTitle: Security Incidents from Lack of Annual Training
Criticality: Medium
PossibleDamage: Increased vulnerability to security incidents, data breaches, and non-compliance per
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to provide annual training may lead to gaps in knowledge, resulting in security
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Send regular reminders for training deadlines", "2": "Offer incentives for completin
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 916:
RiskId: 1860

ComplianceId: 2514
RiskTitle: Outdated Information Security Policy
Criticality: High
PossibleDamage: Data breaches, non-compliance with regulations
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of sensitive data, financial penalties for non-compliance
RiskDescription: Failure to review the Information Security Policy annually may lead to outdated securi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reminders for annual policy review", "2": "Conduct periodic
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 917:
RiskId: 1861
ComplianceId: 2515
RiskTitle: Non-Compliance with Information Security Policy
Criticality: High
PossibleDamage: Potential data breaches, security incidents, and loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to comply with the Information Security Policy can result in unauthorized acce
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on the Information Security Policy", "2": "Email reminde
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 918:
RiskId: 1862
ComplianceId: 2516
RiskTitle: Lack of New Hire Training on Information Security Policy
Criticality: Medium
PossibleDamage: Increased likelihood of security incidents due to new employees' lack of awareness a
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to provide new hires with adequate training on the Information Security Policy
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Incorporating security policy training in the onboarding process", "2": "Assigning m
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 919:
RiskId: 1716
ComplianceId: 2370
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of patient trust and financial penalties

Category: Operational
RiskType: Inherent
BusinessImpact: Operational disruptions and financial losses
RiskDescription: Unauthorized access to ePHI leading to data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for ePHI", "2": "Regularly monitor access logs for unusual a
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 920:
RiskId: 1717
ComplianceId: 2371
RiskTitle: Data Breach Due to Inadequate Security Measures
Criticality: High
PossibleDamage: Data loss, reputational damage, regulatory fines.
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive data, legal consequences, financial penalties.
RiskDescription: Failure to implement appropriate security measures could result in a data breach, lea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security assessments and updates", "2": "Employee training on security p
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 921:
RiskId: 1718
ComplianceId: 2372
RiskTitle: Lack of Documentation Risk
Criticality: High
PossibleDamage: Miscommunication, errors, non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: Potential security breaches and regulatory fines
RiskDescription: Failure to document security measures may result in confusion, errors, and non-comp
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation procedures", "2": "Automated alerts for docum
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 922:
RiskId: 1719
ComplianceId: 2373
RiskTitle: Confusion in Security Responsibilities
Criticality: High
PossibleDamage: Confusion may lead to security gaps and non-compliance with HIPAA Security Rule
Category: Operational
RiskType: Current
BusinessImpact: Potential breaches, data loss, regulatory fines
RiskDescription: Lack of clear security responsibilities may result in mismanagement of security measu

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of security responsibilities", "2": "Training on security r
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 923:
RiskId: 1720
ComplianceId: 2374
RiskTitle: Employee Security Awareness Gap
Criticality: Medium
PossibleDamage: Lack of awareness may result in inadvertent security breaches and data leaks
Category: Operational
RiskType: Current
BusinessImpact: Increased susceptibility to phishing attacks, data breaches
RiskDescription: Insufficient security training may lead to employees unknowingly engaging in risky bel
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a training management system for tracking completion", "2": "Provide r
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 924:
RiskId: 1721

ComplianceId: 2375
RiskTitle: Inaccurate Security Documentation
Criticality: High
PossibleDamage: Inaccurate documentation may result in misapplication of security measures and pot
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of regulatory fines, data exposure
RiskDescription: Outdated or incomplete security documentation may lead to incorrect implementation
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of security documentation", "2": "Implement version co
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 925:
RiskId: 1722
ComplianceId: 2376
RiskTitle: Unauthorized Access to ePHI
Criticality: High
PossibleDamage: Data breaches, compliance violations, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, regulatory fines, legal actions
RiskDescription: Unauthorized individuals gaining access to ePHI due to ineffective access controls, le
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement multi-factor authentication for access control", "2": "Provide regular tra

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 926:

RiskId: 1723

ComplianceId: 2377

RiskTitle: Facility Security Vulnerabilities

Criticality: Medium

PossibleDamage: Security breaches, unauthorized access to ePHI

Category: Operational

RiskType: Current

BusinessImpact: Compromised security of ePHI, potential data breaches

RiskDescription: Physical vulnerabilities in facilities housing ePHI could lead to security breaches and u

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement surveillance systems for monitoring facility security", "2": "Regularly up

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 927:

RiskId: 1724

ComplianceId: 2378

RiskTitle: Data Loss Due to Backup Failure

Criticality: High

PossibleDamage: Data loss, system downtime, inability to recover ePHI

Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, potential data loss
RiskDescription: Failure to perform daily data backups could result in data loss, system downtime, and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated backup systems with redundancy", "2": "Regularly test data
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 928:
RiskId: 1725
ComplianceId: 2379
RiskTitle: Data Breach due to Lack of Encryption
Criticality: High
PossibleDamage: Financial penalties, reputational damage, loss of customer trust
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, legal consequences, loss of business
RiskDescription: Failure to encrypt data at rest and in transit can lead to unauthorized access and disc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption software", "2": "Implement access controls", "3": "Mo
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 929:
RiskId: 1726
ComplianceId: 2380
RiskTitle: Unauthorized Access due to Weak Authentication Controls
Criticality: Medium
PossibleDamage: Data breaches, compromised system integrity, loss of ePHI
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory fines, reputational damage
RiskDescription: Failure to implement strong authentication controls can lead to unauthorized access t
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enforce regular password updates", "2": "Implement biometric authentication", "3"
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 930:
RiskId: 1727
ComplianceId: 2381
RiskTitle: Unauthorized Access to ePHI
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage.
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive information, legal consequences.
RiskDescription: Risk of unauthorized individuals gaining access to ePHI stored in facilities.

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security assessments and audits", "2": "Employee training on security pro
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 931:
RiskId: 1728
ComplianceId: 2382
RiskTitle: Outdated Security Measures
Criticality: Medium
PossibleDamage: Increased vulnerability to security threats, non-compliance with regulations.
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of data breaches, regulatory fines.
RiskDescription: Risk of security measures becoming outdated and ineffective in protecting ePHI.
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update of security plan", "2": "Integration of new security tech
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 932:
RiskId: 1729

ComplianceId: 2383
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: All business units within the organization
RiskDescription: Unauthorized access to ePHI can lead to data breaches, compliance fines, and reputa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enforce strict policies on workstation locking", "2": "Implement automatic screen lo
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 933:
RiskId: 1730
ComplianceId: 2384
RiskTitle: Weak Password Protection Risk
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access to ePHI
Category: IT
RiskType: Residual
BusinessImpact: All business units within the organization
RiskDescription: Weak password protection can lead to unauthorized access to ePHI, data breaches, a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Enforce password complexity requirements", "2": "Implement multi-factor authenti

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 934:

RiskId: 1731

ComplianceId: 2385

RiskTitle: Data Breach Risk

Criticality: High

PossibleDamage: Data breaches, regulatory fines, reputational damage

Category: Compliance

RiskType: Inherent

BusinessImpact: Loss of customer trust, financial penalties, legal consequences

RiskDescription: Unauthorized access to disposed media containing ePHI leading to data breaches an

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strict access controls for media disposal areas", "2": "Encrypt data bef

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 935:

RiskId: 1732

ComplianceId: 2386

RiskTitle: Data Wiping Risk

Criticality: Medium

PossibleDamage: Unauthorized access to ePHI due to incomplete data wiping

Category: IT
RiskType: Inherent
BusinessImpact: Loss of sensitive information, compliance violations
RiskDescription: Incomplete data wiping on media containing ePHI leading to unauthorized access and
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated data wiping processes", "2": "Regularly test data wiping effe
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 936:
RiskId: 1733
ComplianceId: 2387
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, legal consequences
RiskDescription: Unauthorized users gaining access to ePHI leading to data breaches and compliance
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Enforce multi-factor authentication", "3
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 937:
RiskId: 1734
ComplianceId: 2388
RiskTitle: Outdated Access Levels Risk
Criticality: Medium
PossibleDamage: Unauthorized access, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Risk of unauthorized access and compliance violations
RiskDescription: Outdated user access levels leading to unauthorized access and compliance violation
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review user access levels", "2": "Implement access level change approv
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 938:
RiskId: 1735
ComplianceId: 2389
RiskTitle: Data Breach Due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive ePHI, reputational damage, regulatory fines.
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, legal consequences.
RiskDescription: Unauthorized access to ePHI can lead to data breaches and significant consequence

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls and regular monitoring", "2": "Encrypt sensitive
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 939:
RiskId: 1736
ComplianceId: 2390
RiskTitle: Compromise of ePHI Integrity
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, legal implications
RiskDescription: Unauthorized access to ePHI, data manipulation, data corruption leading to breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly perform data integrity checks during data entry and thereafter", "2": "Im
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 940:
RiskId: 1737

ComplianceId: 2391
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Exposure of sensitive ePHI and regulatory penalties
Category: IT
RiskType: Inherent
BusinessImpact: Disruption of operations, loss of trust from stakeholders
RiskDescription: Unauthorized access to ePHI leading to data breach and potential legal consequence
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for ePHI data at rest and in transit", "2": "Regularly monitor
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 941:
RiskId: 1738
ComplianceId: 2392
RiskTitle: Failure to Implement Security Measures within 90 days
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, Legal consequences
RiskDescription: Failure to implement security measures within the specified timeframe could expose t
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear implementation timelines", "2": "Regularly review progress and adj

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 942:

RiskId: 1739

ComplianceId: 2393

RiskTitle: Inadequate Documentation of Security Measures Implementation

Criticality: Medium

PossibleDamage: Confusion, non-compliance, inefficiencies

Category: Operational

RiskType: Current

BusinessImpact: Difficulty in tracking compliance, Inefficient security measures implementation

RiskDescription: Lack of clear documentation on the implementation of security measures may lead to

RiskLikelihood: 7

RiskImpact: 6

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement standardized documentation templates", "2": "Conduct regular audits c

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 943:

RiskId: 1740

ComplianceId: 2394

RiskTitle: Unauthorized Access to ePHI

Criticality: High

PossibleDamage: Unauthorized access to ePHI can lead to data breaches and legal consequences.

Category: Operational
RiskType: Current
BusinessImpact: Disruption of services, loss of trust, legal penalties
RiskDescription: Unauthorized individuals gaining access to sensitive ePHI due to undocumented secu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls", "2": "Regularly review access logs", "3": "Encrypt ser
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 944:
RiskId: 1741
ComplianceId: 2395
RiskTitle: Outdated Security Practices
Criticality: Medium
PossibleDamage: Outdated security practices may not effectively protect against current threats.
Category: Operational
RiskType: Current
BusinessImpact: Increased vulnerability to cyber attacks
RiskDescription: Failure to review security practices annually may result in outdated measures that are
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular security training for staff", "2": "Implement threat intelligence monitoring",
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 945:
RiskId: 1742
ComplianceId: 2396
RiskTitle: Unauthorized Access to ePHI
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential disruption of operations, financial losses, legal liabilities
RiskDescription: Unauthorized access to ePHI can lead to data breaches, compromising patient privac
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls and encryption", "2": "Regularly monitor access
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 946:
RiskId: 1743
ComplianceId: 2397
RiskTitle: Human Error in Handling ePHI
Criticality: Medium
PossibleDamage: Data breaches, non-compliance penalties, reputational harm
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of patient trust, regulatory fines, legal consequences
RiskDescription: Lack of security training may lead to inadvertent disclosure of ePHI, resulting in data b

RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update training content based on evolving threats", "2": "Conduct simul
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 947:
RiskId: 1744
ComplianceId: 2398
RiskTitle: Unauthorized Access to ePHI Storage Areas
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, legal consequences
RiskDescription: Unauthorized individuals gaining access to ePHI storage areas can lead to data brea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for access control", "2": "Regularly update a
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 948:
RiskId: 1745

ComplianceId: 2399
RiskTitle: Data Loss Due to Lack of Off-Site Backups
Criticality: Medium
PossibleDamage: Operational disruptions, data loss, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Loss of critical data, financial losses, reputational damage
RiskDescription: Failure to maintain off-site backups can result in data loss during environmental hazar
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate off-site backup processes for consistency", "2": "Regularly test data rec
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 949:
RiskId: 1746
ComplianceId: 2400
RiskTitle: Unauthorized Access to ePHI
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, legal consequences
RiskDescription: Unauthorized individuals gaining access to ePHI data through weak authentication co
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on proper authentication procedures", "2": "Implementing strong

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 950:

RiskId: 1747

ComplianceId: 2401

RiskTitle: Data Interception due to Outdated Encryption Protocols

Criticality: Medium

PossibleDamage: Exposure of sensitive ePHI, compliance violations

Category: IT

RiskType: Residual

BusinessImpact: Loss of data confidentiality, regulatory fines

RiskDescription: Attackers intercepting data transmissions due to outdated encryption protocols, leadir

RiskLikelihood: 6

RiskImpact: 8

RiskExposureRating: 48

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly review encryption protocols for vulnerabilities", "2": "Implement automat

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 951:

RiskId: 1748

ComplianceId: 2402

RiskTitle: Data Breach Risk

Criticality: High

PossibleDamage: Loss of sensitive information, regulatory fines

Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, reputational damage
RiskDescription: Unauthorized access to ePHI leading to data breach
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for ePHI", "2": "Implement multi-factor authentication", "3": '
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 952:
RiskId: 1749
ComplianceId: 2403
RiskTitle: System Downtime Risk
Criticality: Medium
PossibleDamage: Disruption of operations, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Loss of productivity, revenue impact
RiskDescription: Significant IT environment changes leading to system downtime
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement backup and recovery procedures", "2": "Test changes in a controlled e
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 953:
RiskId: 1750
ComplianceId: 2404
RiskTitle: Delayed Implementation of Security Measures
Criticality: High
PossibleDamage: Unauthorized access to ePHI
Category: IT
RiskType: Current
BusinessImpact: Potential data breach and regulatory fines
RiskDescription: Failure to implement security measures within 90 days may expose systems to cyber
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting of progress", "2": "Escalation process for delays
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 954:
RiskId: 1751
ComplianceId: 2405
RiskTitle: Ineffective Security Measure Selection
Criticality: Medium
PossibleDamage: Wastage of resources on ineffective security measures
Category: IT
RiskType: Current
BusinessImpact: Inefficient use of resources and potential data breaches
RiskDescription: Selection of security measures solely based on cost without considering effectiveness

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Cost-benefit analysis for each security measure", "2": "Pilot testing before full imp
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 955:
RiskId: 1752
ComplianceId: 2406
RiskTitle: Risk of Inadequate Documentation
Criticality: High
PossibleDamage: Potential security breaches, data loss, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust, financial losses
RiskDescription: Failure to document security measures may result in gaps in security understanding,
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation procedures", "2": "Automated reminders for do
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 956:
RiskId: 1753

ComplianceId: 2407
RiskTitle: Risk of Ineffective Security Measures
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats, data breaches, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust, financial losses
RiskDescription: Failure to review security measures annually may result in outdated controls that are
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear review criteria", "2": "Automate review scheduling and notifications
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 957:
RiskId: 1754
ComplianceId: 2408
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of sensitive information, reputational damage, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: All business units handling ePHI
RiskDescription: Unauthorized access to ePHI leading to data breaches and potential legal consequen
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly monitor access logs", "3": "

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 958:

RiskId: 1755

ComplianceId: 2409

RiskTitle: Phishing Attacks Targeting New Hires

Criticality: Medium

PossibleDamage: Loss of sensitive data, reputational damage

Category: Operational

RiskType: Residual

BusinessImpact: Disruption to operations, potential financial loss

RiskDescription: New employees may not be adequately trained to identify phishing attempts, leading t

RiskLikelihood: 7

RiskImpact: 8

RiskExposureRating: 56

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement email filtering to catch phishing emails", "2": "Provide ongoing phishing

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 959:

RiskId: 1756

ComplianceId: 2410

RiskTitle: Social Engineering Attacks Due to Lack of Training

Criticality: High

PossibleDamage: Loss of sensitive data, financial loss

Category: Operational
RiskType: Residual
BusinessImpact: Disruption to operations, reputational damage
RiskDescription: Employees may be susceptible to social engineering tactics if not regularly trained on
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for sensitive systems", "2": "Conduct simula
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 960:
RiskId: 1757
ComplianceId: 2411
RiskTitle: Unauthorized Access to ePHI Facilities
Criticality: High
PossibleDamage: Data breaches, non-compliance penalties
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, legal consequences
RiskDescription: Unauthorized individuals gaining access to facilities housing ePHI, leading to potentia
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access control lists", "2": "Implement multi-factor aut
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 961:
RiskId: 1758
ComplianceId: 2412
RiskTitle: Inadequate Surveillance Monitoring
Criticality: Medium
PossibleDamage: Security breaches, unauthorized access
Category: Operational
RiskType: Current
BusinessImpact: Security incidents going undetected, potential data breaches
RiskDescription: Lack of effective surveillance monitoring leading to potential security breaches and un
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review surveillance footage for any suspicious activities", "2": "Ensure c
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 962:
RiskId: 1759
ComplianceId: 2413
RiskTitle: Unauthorized Access to ePHI
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial penalties, legal consequences
RiskDescription: Unauthorized access to ePHI can lead to data breaches, regulatory fines, and reputat

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular assessment of workstation security measures", "2": "Employee training o
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 963:
RiskId: 1760
ComplianceId: 2414
RiskTitle: Risk of Unauthorized Access to ePHI
Criticality: High
PossibleDamage: Unauthorized access to sensitive patient data
Category: Operational
RiskType: Current
BusinessImpact: Potential legal consequences and damage to reputation
RiskDescription: Failure to implement multi-factor authentication may lead to unauthorized access to e
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review access logs for suspicious activity", "2": "Implement biometric au
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 964:
RiskId: 1761

ComplianceId: 2415
RiskTitle: Risk of Outdated Access Controls
Criticality: Medium
PossibleDamage: Unauthorized access to ePHI due to outdated access controls
Category: Operational
RiskType: Current
BusinessImpact: Potential compliance violations and data breaches
RiskDescription: Failure to regularly review and update access controls may result in outdated permiss
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update access control lists", "2": "Implement automated acc
CreatedAt: 2025-10-29 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 965:
RiskId: 1762
ComplianceId: 2416
RiskTitle: Unauthorized Access to ePHI Data
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory penalties, damage to reputation
RiskDescription: Unauthorized access to encrypted ePHI data can lead to data breaches, regulatory fi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly review and update encryption protocols", "2": "Implement multi-factor au

CreatedAt: 2025-10-29 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 966:

RiskId: 1715

ComplianceId: 2369

RiskTitle: mmmmmmmmmmmmmmmmmmmmm

Criticality: Medium

PossibleDamage: mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm

Category: People Risk

RiskType: Current

BusinessImpact: Customer Impact

RiskDescription: mmmmmmmmmmmmmmmmmmmmmmmmmmmmm

RiskLikelihood: 5

RiskImpact: 8

RiskExposureRating: 40

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: None

CreatedAt: 2025-10-28 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 967:

RiskId: 1617

ComplianceId: 2269

RiskTitle: Data Breach Risk

Criticality: High

PossibleDamage: Financial losses, reputational damage

Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Risk of unauthorized access to sensitive data leading to data breaches
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption protocols", "2": "Enforce access controls", "3": "Regular sec
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 968:
RiskId: 1618
ComplianceId: 2270
RiskTitle: Outdated Controls Risk
Criticality: Medium
PossibleDamage: Vulnerabilities, non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Increased risk exposure, regulatory fines
RiskDescription: Risk of using outdated security controls leading to vulnerabilities and non-compliance
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular updates and patches", "2": "Continuous monitoring", "3": "Training and av
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 969:
RiskId: 1619
ComplianceId: 2271
RiskTitle: Unidentified Technology Risks
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Failure to conduct quarterly risk assessments may result in unidentified technology ris
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated risk assessment tools", "2": "Provide regular training on risk
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 970:
RiskId: 1620
ComplianceId: 2272
RiskTitle: Inadequate Board Oversight
Criticality: Medium
PossibleDamage: Increased exposure to risks
Category: Operational
RiskType: Inherent
BusinessImpact: Inadequate decision-making, increased exposure to threats
RiskDescription: Failure to report technology risks to the board may result in inadequate oversight lead

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting procedures", "2": "Provide training on effective communi
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 971:
RiskId: 1621
ComplianceId: 2273
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of sensitive information, reputational damage
Category: IT
RiskType: Inherent
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Unauthorized access to sensitive data due to security vulnerabilities
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for sensitive data", "2": "Implement multi-factor authenticati
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 972:
RiskId: 1622

ComplianceId: 2274
RiskTitle: Change Management Risk
Criticality: Medium
PossibleDamage: Service disruptions, data loss
Category: IT
RiskType: Inherent
BusinessImpact: Operational delays, financial losses
RiskDescription: Uncontrolled changes leading to system instability or data corruption
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement change control board for approvals", "2": "Test changes in isolated env
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 973:
RiskId: 1623
ComplianceId: 2275
RiskTitle: Failure to Implement Technology Risk Mitigation Strategies
Criticality: High
PossibleDamage: Data breaches, system downtime, financial losses
Category: IT
RiskType: Current
BusinessImpact: IT Security Team, Data Management Team
RiskDescription: Failure to implement risk mitigation strategies within the specified timeframe may exp
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular monitoring of risk management frameworks", "2": "Quarterly review of imp

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 974:

RiskId: 1624

ComplianceId: 2276

RiskTitle: Lack of Oversight by Chief Information Officer

Criticality: High

PossibleDamage: Inadequate oversight leading to increased technology risks

Category: Operational

RiskType: Current

BusinessImpact: Potential disruptions to technology operations and increased vulnerability to cyber thr

RiskDescription: Failure to appoint a qualified Chief Information Officer may result in inadequate oversi

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular reporting and monitoring of technology risk metrics", "2": "Implementing r

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 975:

RiskId: 1625

ComplianceId: 2277

RiskTitle: Inadequate Skills in Technology Risk Officers

Criticality: Medium

PossibleDamage: Lack of expertise leading to increased technology risks

Category: Operational
RiskType: Current
BusinessImpact: Potential gaps in technology risk management processes and increased vulnerability
RiskDescription: Appointing unqualified individuals to technology risk officer roles may result in inadequ
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Providing ongoing training and development opportunities for technology risk offic
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 976:
RiskId: 1626
ComplianceId: 2278
RiskTitle: Failure to Establish Technology Risk Management Framework
Criticality: High
PossibleDamage: Increased technology-related risks, potential data breaches, and financial losses
Category: IT
RiskType: Current
BusinessImpact: All business units would be impacted by potential technology-related risks
RiskDescription: The absence of a comprehensive technology risk management framework may expos
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting on the progress of framework implementation",
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 977:
RiskId: 1627
ComplianceId: 2279
RiskTitle: Outdated Technology Risk Management Strategy
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats, potential financial losses
Category: IT
RiskType: Residual
BusinessImpact: All business units would be impacted by potential breaches or data loss
RiskDescription: Failure to update the technology risk management strategy could result in outdated co
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reviews and updates of the strategy", "2": "Continuous monitoring of tech
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 978:
RiskId: 1628
ComplianceId: 2280
RiskTitle: Inadequate Audit of Technology Risk Management
Criticality: High
PossibleDamage: Undetected weaknesses in the technology risk management strategy, regulatory non
Category: IT
RiskType: Residual
BusinessImpact: All business units would be impacted by undetected weaknesses in the strategy
RiskDescription: Failure to conduct thorough audits could result in unidentified vulnerabilities and non-c

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance audit procedures", "2": "Implement continuous monitoring controls", "3":
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 979:
RiskId: 1629
ComplianceId: 2281
RiskTitle: Inadequate Technology Leadership
Criticality: High
PossibleDamage: Increased technology risks, security breaches, and regulatory non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: Technology Management
RiskDescription: Failure to appoint qualified individuals in key technology leadership roles may result in
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify qualifications and experience of appointed individuals", "2": "Provide ongoi
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 980:
RiskId: 1630

ComplianceId: 2282
RiskTitle: Inadequate Selection Process for Technology Leadership Roles
Criticality: Medium
PossibleDamage: Increased technology risks and security vulnerabilities
Category: Operational
RiskType: Inherent
BusinessImpact: Technology Management
RiskDescription: An inadequate selection process for key technology leadership roles may result in unc
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear selection criteria and evaluation metrics", "2": "Involve multiple sta
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 981:
RiskId: 1631
ComplianceId: 2283
RiskTitle: Failure to Establish Technology Risk Management Framework
Criticality: High
PossibleDamage: Increased vulnerability to technology-related risks and potential financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: All business units could face disruptions and financial losses
RiskDescription: The lack of a structured risk management framework increases the likelihood of techn
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting on the implementation progress", "2": "Engagem
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 982:
RiskId: 1632
ComplianceId: 2284
RiskTitle: Failure to Conduct Annual Review of Technology Risk Management Framework
Criticality: Medium
PossibleDamage: Outdated risk management practices and increased exposure to emerging threats
Category: IT
RiskType: Inherent
BusinessImpact: Technology operations and departments could face disruptions and compliance issue
RiskDescription: Without regular reviews, the technology risk management framework may not addres
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a formal review process with defined timelines and responsibilities", "2":
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 983:
RiskId: 1633
ComplianceId: 2285
RiskTitle: Lack of Technology Risk Awareness
Criticality: High
PossibleDamage: Increased vulnerability to technology-related incidents and breaches

Category: Operational
RiskType: Current
BusinessImpact: All business units may be impacted by staff unawareness of technology risks
RiskDescription: Failure to conduct regular training may result in staff being unaware of current techno
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update training materials to reflect current technology risks", "2": "Provi
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 984:
RiskId: 1634
ComplianceId: 2286
RiskTitle: Inadequate Training Materials
Criticality: Medium
PossibleDamage: Inadequate training materials may result in staff not fully understanding technology r
Category: Operational
RiskType: Current
BusinessImpact: Human Resources and IT Security teams may be impacted by inadequate training ma
RiskDescription: Inadequate training materials may result in staff not fully understanding technology ris
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update training materials based on emerging technology ris
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 985:
RiskId: 1635
ComplianceId: 2287
RiskTitle: Unidentified Risks due to Lack of Assessment
Criticality: High
PossibleDamage: Potential regulatory violations and financial losses
Category: Operational
RiskType: Residual
BusinessImpact: All business units involved in technology risk management
RiskDescription: Failure to conduct risk assessments may result in unidentified risks that could lead to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training for the Risk Management Team on risk assessment te
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 986:
RiskId: 1636
ComplianceId: 2288
RiskTitle: Non-Compliance Risk
Criticality: High
PossibleDamage: Increased risk of non-compliance penalties, reputational damage, and operational di
Category: Compliance
RiskType: Residual
BusinessImpact: All business units would be impacted by non-compliance risks
RiskDescription: Failure to comply with established policies and standards could result in financial pena

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on compliance requirements", "2": "Imp
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 987:
RiskId: 1637
ComplianceId: 2289
RiskTitle: Non-Compliance Resolution Risk
Criticality: Medium
PossibleDamage: Continued non-compliance, escalation of penalties, and reputational harm
Category: Compliance
RiskType: Residual
BusinessImpact: All business units would be impacted by non-compliance risks
RiskDescription: Failure to promptly address instances of non-compliance could lead to ongoing violati
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear escalation procedures for unresolved non-compliance issues", "2"
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 988:
RiskId: 1638

ComplianceId: 2290
RiskTitle: Inaccurate Asset Classification
Criticality: High
PossibleDamage: Data breaches, loss of critical information
Category: Operational
RiskType: Residual
BusinessImpact: IT, Legal, Compliance
RiskDescription: Failure to conduct regular audits may lead to inaccurate classification of assets, increa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated audit tools for regular asset identification", "2": "Provide trai
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 989:
RiskId: 1639
ComplianceId: 2291
RiskTitle: Miscommunication and Lack of Accountability
Criticality: High
PossibleDamage: Miscommunication, errors, and security breaches
Category: Operational
RiskType: Residual
BusinessImpact: All departments involved in information asset management
RiskDescription: Misunderstanding of roles and responsibilities can lead to miscommunication, errors,
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on RACI matrix understanding", "2": "Periodic reviews of RACI m

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 990:

RiskId: 1640

ComplianceId: 2292

RiskTitle: Data Breach from Third Party

Criticality: High

PossibleDamage: Loss of sensitive data, financial penalties, reputational damage

Category: Operational

RiskType: Residual

BusinessImpact: All business units

RiskDescription: Inadequate third party risk assessment may result in a data breach compromising ser

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement encryption for data transfer", "2": "Regularly monitor third party securit

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 991:

RiskId: 1641

ComplianceId: 2293

RiskTitle: Inadequate Competency in IT Roles

Criticality: High

PossibleDamage: Inefficient IT operations, increased security vulnerabilities, and potential financial los

Category: Operational
RiskType: Residual
BusinessImpact: Potential delays in project delivery, increased likelihood of errors and security breach
RiskDescription: Hiring personnel without the required competencies can lead to operational inefficienc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement standardized evaluation forms and reference checks", "2": "Provide tar
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 992:
RiskId: 1642
ComplianceId: 2294
RiskTitle: Lack of Collaborative Competency Assessment
Criticality: Medium
PossibleDamage: Incomplete assessments, overlooking critical competencies, and suboptimal IT perfo
Category: Operational
RiskType: Residual
BusinessImpact: Potential performance issues in IT functions due to incomplete competency assessm
RiskDescription: Failure to collaborate in competency assessments may lead to overlooking critical co
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels between HR and IT management", "2": "
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 993:
RiskId: 1643
ComplianceId: 2295
RiskTitle: Risk of Hiring Individuals with Criminal Records
Criticality: High
PossibleDamage: Potential security breaches, data theft, or fraudulent activities
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, damage to reputation, financial losses
RiskDescription: Hiring individuals with criminal records increases the risk of security breaches and fra
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict background check policies", "2": "Provide ongoing security trainin
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 994:
RiskId: 1644
ComplianceId: 2296
RiskTitle: Risk of Hiring Individuals with False Employment History
Criticality: Medium
PossibleDamage: Potential mismatch between job requirements and personnel skills/experience
Category: Operational
RiskType: Current
BusinessImpact: Decreased organizational performance, increased turnover rates
RiskDescription: Hiring individuals with false employment history may result in unqualified personnel oc

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement robust reference check processes", "2": "Provide training to HR staff o
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 995:
RiskId: 1645
ComplianceId: 2297
RiskTitle: Non-Compliance with Annual Security Awareness Training
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats, potential data breaches, and non-complianc
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential data breaches and cybersecurity in
RiskDescription: Failure to conduct annual security awareness training may result in staff, contractors,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training attendance", "2": "Implementing quizzes or assessr
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 996:
RiskId: 1646

ComplianceId: 2300
RiskTitle: Inadequate Training Program Content
Criticality: High
PossibleDamage: Increased vulnerability to security threats and non-compliance with policies
Category: Operational
RiskType: Current
BusinessImpact: Reduced security posture and potential regulatory fines or penalties
RiskDescription: Outdated training content may result in employees lacking the necessary knowledge a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update training materials based on review findings", "2": "Provide additi
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 997:
RiskId: 1647
ComplianceId: 2301
RiskTitle: Unidentified Technology Risks
Criticality: High
PossibleDamage: Potential security breaches, system failures, or data loss
Category: IT
RiskType: Inherent
BusinessImpact: Operational disruptions, financial losses, reputational damage
RiskDescription: Failure to conduct annual risk assessments may result in unidentified technology risks
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training on risk assessment procedures", "2": "Implementing automated r
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 998:
RiskId: 1648
ComplianceId: 2302
RiskTitle: Failure to Develop and Implement Risk Mitigation Strategies
Criticality: High
PossibleDamage: Increased vulnerability to technology risks, potential data breaches, and system failu
Category: Operational
RiskType: Current
BusinessImpact: All business units involved in technology management may experience disruptions ar
RiskDescription: Failure to develop and implement risk mitigation strategies within the specified timelin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular risk assessments to identify new risks", "2": "Continuous monitoring of im
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 999:
RiskId: 1649
ComplianceId: 2303
RiskTitle: Lack of Clear Risk Ownership
Criticality: High
PossibleDamage: Ineffective risk management, potential technology failures

Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of technology operations, financial losses
RiskDescription: Failure to assign risk owners may result in unclear accountability, leading to delays in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and communication on risk ownership responsibilities", "2": "Peri
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1000:
RiskId: 1650
ComplianceId: 2304
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of customer trust, financial penalties
Category: IT
RiskType: Residual
BusinessImpact: IT systems and customer data
RiskDescription: Unauthorized access to sensitive data due to inadequate risk assessments
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Encrypt sensitive data at rest and in t
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1001:
RiskId: 1651
ComplianceId: 2305
RiskTitle: Treatment Plan Update Risk
Criticality: Medium
PossibleDamage: Increased vulnerability to cyber threats
Category: IT
RiskType: Residual
BusinessImpact: IT systems and data integrity
RiskDescription: Failure to update treatment plans based on risk assessment findings
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated risk monitoring tools", "2": "Establish clear escalation proce
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1002:
RiskId: 1652
ComplianceId: 2306
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of sensitive information, financial losses, and reputational damage
Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, legal consequences
RiskDescription: The risk of unauthorized access to sensitive data due to unaddressed vulnerabilities

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for sensitive data", "2": "Regularly update security policies a
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1003:
RiskId: 1653
ComplianceId: 2307
RiskTitle: Outdated Risk Treatment Plans
Criticality: High
PossibleDamage: Ineffective risk mitigation strategies and increased vulnerability to risks
Category: Operational
RiskType: Current
BusinessImpact: All business units within the organization
RiskDescription: Failure to update risk treatment plans annually may result in outdated strategies that c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear schedule for annual reviews", "2": "Ensure active participation of
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1004:
RiskId: 1654

ComplianceId: 2308
RiskTitle: Incomplete Risk Register
Criticality: High
PossibleDamage: Unidentified risks may lead to financial losses or operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Risk Management Team and all organizational units
RiskDescription: Failure to maintain a comprehensive risk register may result in unidentified risks that c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for the Risk Management Team on risk identification and docume
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1005:
RiskId: 1655
ComplianceId: 2309
RiskTitle: Lack of Quarterly Reporting
Criticality: High
PossibleDamage: Uninformed decision-making by senior management leading to financial or reputatio
Category: Operational
RiskType: Current
BusinessImpact: Risk Management Team, Senior Management, and all organizational units
RiskDescription: Failure to provide quarterly reports to senior management may result in uninformed d
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting templates for consistency", "2": "Schedule regular meeti
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1006:
RiskId: 1656
ComplianceId: 2310
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Financial loss, reputational damage
Category: IT
RiskType: Current
BusinessImpact: Loss of customer trust, legal liabilities
RiskDescription: Unauthorized access to sensitive data leading to data breaches and financial losses
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption and access controls", "2": "Regularly monitor and audit syst
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1007:
RiskId: 1657
ComplianceId: 2311
RiskTitle: Increased Vulnerability to Cyber Threats
Criticality: High
PossibleDamage: Potential data breaches and compromised information assets

Category: IT
RiskType: Residual
BusinessImpact: IT Security Team, Risk Management Team
RiskDescription: Failure to implement effective risk mitigation measures may lead to increased vulnera
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of risk mitigation strategies", "2": "Implementation of s
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1008:
RiskId: 1658
ComplianceId: 2312
RiskTitle: Incomplete Risk Register
Criticality: High
PossibleDamage: Undetected technology risks may lead to significant financial losses and reputationa
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face disruptions or losses due to unidentified risks.
RiskDescription: Failure to maintain a comprehensive risk register may result in critical technology risk
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update the risk register with new risks and their assessments", "2": "Co
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1009:
RiskId: 1659
ComplianceId: 2313
RiskTitle: Delayed Risk Reporting
Criticality: High
PossibleDamage: Delayed reporting of significant risks may lead to missed opportunities for timely risk
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face increased exposure to threats due to delayed risk reportin
RiskDescription: Failure to report significant technology risks on a quarterly basis may result in key sta
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting templates and guidelines for consistent reporting", "2": "C
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1010:
RiskId: 1660
ComplianceId: 2314
RiskTitle: Ineffective Risk Mitigation Measures
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: All business units managing information assets
RiskDescription: Failure to update risk mitigation measures may leave the organization vulnerable to k

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update risk mitigation measures", "2": "Engage key stakeho
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1011:
RiskId: 1661
ComplianceId: 2315
RiskTitle: Unidentified Technology Risks
Criticality: High
PossibleDamage: Potential security breaches or system failures
Category: IT
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to maintain a risk register may lead to unidentified technology risks that could
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on risk register maintenance procedures", "2": "Implement autom
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1012:
RiskId: 1662

ComplianceId: 2316
RiskTitle: Delayed Risk Reporting
Criticality: Medium
PossibleDamage: Increased exposure to potential threats
Category: IT
RiskType: Inherent
BusinessImpact: Risk management team and compliance officers
RiskDescription: Delay in reporting significant risks may result in stakeholders being unaware of potent
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting timelines and escalation procedures", "2": "Automate rep
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1013:
RiskId: 1663
ComplianceId: 2317
RiskTitle: Outdated Risk Register
Criticality: High
PossibleDamage: Failure to update the risk register regularly may result in outdated risk information lea
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by ineffective risk management strategies.
RiskDescription: Failure to update the risk register regularly may result in outdated risk information, lea
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish automated reminders for quarterly reviews", "2": "Provide regular trainin

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1014:

RiskId: 1664

ComplianceId: 2318

RiskTitle: Inconsistent Risk Information

Criticality: Medium

PossibleDamage: Inconsistent or incomplete risk information may lead to misinterpretation of risks and

Category: IT

RiskType: Residual

BusinessImpact: Risk Management Department would be impacted by misinterpretation of risks and in

RiskDescription: Inconsistent or incomplete risk information in the risk register may lead to misinterpret

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Provide training to staff on the proper use of the standardized template", "2": "Imp

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 1015:

RiskId: 1665

ComplianceId: 2319

RiskTitle: Failure to Conduct Security Assessment

Criticality: High

PossibleDamage: Potential data breaches, financial losses, reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: All business units involved in the IT project may suffer financial losses and reputation
RiskDescription: Failure to conduct security assessments may result in unidentified security risks, pote
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular security training for project managers and security teams", "2":
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1016:
RiskId: 1666
ComplianceId: 2320
RiskTitle: Failure to Implement Security Controls
Criticality: High
PossibleDamage: Unauthorized access, data breaches, compromise of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: All business units involved in the project may suffer financial losses, reputational dam
RiskDescription: Failure to implement security controls as per the security plan may result in unauthori
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security training for project teams", "2": "Continuous monitoring and testi
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1017:
RiskId: 1667
ComplianceId: 2321
RiskTitle: Increased Vulnerability to Security Breaches
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, financial loss, reputational damage
RiskDescription: Failure to conduct quarterly security control reviews may result in undetected vulneral
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools", "2": "Regularly update security controls b
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1018:
RiskId: 1668
ComplianceId: 2322
RiskTitle: Misalignment of Security Controls with Project Changes
Criticality: Medium
PossibleDamage: Increased vulnerability to security threats, potential security incidents
Category: IT
RiskType: Residual
BusinessImpact: Operational disruptions, financial loss
RiskDescription: Failure to review security controls after significant project changes may lead to misalig

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement change management processes to trigger security control reviews", "2
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1019:
RiskId: 1669
ComplianceId: 2323
RiskTitle: IT Project Plan Deviation Risk
Criticality: High
PossibleDamage: Project delays, cost overruns, and quality issues
Category: Operational
RiskType: Inherent
BusinessImpact: Impact on project timelines, budget, and stakeholder satisfaction
RiskDescription: Deviation from the project plan can lead to delays in project delivery, increased costs,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular project status meetings to identify deviations early", "2": "Implement char
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1020:
RiskId: 1670

ComplianceId: 2324
RiskTitle: Unapproved IT Project Plan Risk
Criticality: Medium
PossibleDamage: Commencement of projects without clear direction
Category: Operational
RiskType: Inherent
BusinessImpact: Rework, delays, and potential stakeholder dissatisfaction
RiskDescription: Starting a project without an approved plan can lead to misunderstandings, rework, a
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear approval process for project plans", "2": "Ensure key stakeholders
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1021:
RiskId: 1671
ComplianceId: 2325
RiskTitle: Inaccurate Feasibility Analysis
Criticality: High
PossibleDamage: Budget overruns and project delays
Category: Operational
RiskType: Residual
BusinessImpact: IT Department
RiskDescription: Proceeding with a project based on inaccurate feasibility analysis can result in misallo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Conduct thorough feasibility analysis with input from all stakeholders", "2": "Imple

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 1022:

RiskId: 1672

ComplianceId: 2326

RiskTitle: Outdated Project Plan

Criticality: Medium

PossibleDamage: Project delays and cost overruns

Category: Operational

RiskType: Residual

BusinessImpact: IT Department

RiskDescription: Proceeding with an outdated project plan can result in missed deadlines, misallocated

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly update the project plan based on project progress", "2": "Conduct regul

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1023:

RiskId: 1673

ComplianceId: 2327

RiskTitle: Failure to Implement Risk Management Process

Criticality: High

PossibleDamage: Project delays, cost overruns, or project failure

Category: Operational
RiskType: Inherent
BusinessImpact: Significant impact on project timelines and budgets
RiskDescription: Failure to implement a risk management process may result in unidentified risks caus
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on risk management processes", "2": "Regular risk assessments
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1024:
RiskId: 1674
ComplianceId: 2328
RiskTitle: Ineffective Oversight of Large Projects
Criticality: High
PossibleDamage: Project delays, budget overruns, failure to meet objectives
Category: Operational
RiskType: Inherent
BusinessImpact: All business units involved in the project may be impacted.
RiskDescription: Lack of oversight from a Steering Committee may lead to misalignment of project goa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear project objectives and success criteria", "2": "Regularly review pro
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1025:
RiskId: 1675
ComplianceId: 2329
RiskTitle: Infrequent Steering Committee Meetings
Criticality: Medium
PossibleDamage: Delayed decisions, misalignment of goals, inadequate progress tracking
Category: Operational
RiskType: Inherent
BusinessImpact: Projects overseen by the Steering Committee may face delays and resource constrai
RiskDescription: Lack of regular meetings may lead to missed opportunities for course correction, dela
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear meeting objectives and outcomes", "2": "Assign action items with c
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1026:
RiskId: 1676
ComplianceId: 2330
RiskTitle: Failure to Escalate Critical Risks
Criticality: High
PossibleDamage: Project delays, cost overruns, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Delays in project delivery, increased costs, damage to organizational reputation
RiskDescription: Failure to escalate critical risks in a timely manner may result in project failures or fina

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear escalation guidelines and procedures", "2": "Regular monitoring of
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1027:
RiskId: 1677
ComplianceId: 2331
RiskTitle: Inadequate Vendor Evaluation Documentation
Criticality: High
PossibleDamage: Biased vendor selection decisions, disputes with vendors
Category: Operational
RiskType: Current
BusinessImpact: Delays in project timelines, increased project costs, damage to vendor relationships
RiskDescription: Failure to document vendor evaluations properly may result in inaccurate decision-ma
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation standards", "2": "Peer review of evaluation doc
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1028:
RiskId: 1678

ComplianceId: 2332
RiskTitle: Vendor Evaluation Timeline Non-Adherence
Criticality: Medium
PossibleDamage: Delayed project timelines, rushed decisions
Category: Operational
RiskType: Current
BusinessImpact: Increased project costs, compromised project quality, potential project failures
RiskDescription: Failure to adhere to vendor evaluation timelines may result in rushed decisions, delay
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular progress tracking and reporting", "2": "Escalation procedures for delays",
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1029:
RiskId: 1679
ComplianceId: 2333
RiskTitle: Late Discovery of Security Requirements
Criticality: High
PossibleDamage: Security vulnerabilities and breaches during development
Category: IT
RiskType: Inherent
BusinessImpact: IT, Security
RiskDescription: Failure to identify and document security requirements early in the SDLC may result i
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular reviews of security requirements with stakeholders", "2": "Training for pro
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1030:
RiskId: 1680
ComplianceId: 2334
RiskTitle: Undetected Security Vulnerabilities
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Failure to detect security vulnerabilities can result in unauthorized access to sensitive
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular security assessments", "2": "Train project teams on secure coc
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1031:
RiskId: 1681
ComplianceId: 2335
RiskTitle: Inaccurate Requirements Documentation
Criticality: High
PossibleDamage: Project delays, cost overruns, and system failures

Category: Operational
RiskType: Residual
BusinessImpact: Delays in project timelines, increased costs, and potential negative impact on busines
RiskDescription: Failure to accurately document requirements may result in system functionalities not r
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reviews of documentation by project stakeholders", "2": "Training for proj
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1032:
RiskId: 1682
ComplianceId: 2336
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Potential legal consequences and loss of customer trust
RiskDescription: Unauthorized access to sensitive data due to inadequate security measures
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for sensitive data", "2": "Implement multi-factor authenticati
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1033:
RiskId: 1683
ComplianceId: 2337
RiskTitle: Non-compliant IT System Implementation
Criticality: High
PossibleDamage: Security breaches, data loss, system failures
Category: IT
RiskType: Current
BusinessImpact: Disruption of IT operations, financial losses, reputational damage
RiskDescription: Failure to conduct design reviews may result in the implementation of IT systems that
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear review schedule and assign responsibilities", "2": "Provide trainin
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1034:
RiskId: 1684
ComplianceId: 2338
RiskTitle: Inadequate Test Plan Development
Criticality: High
PossibleDamage: Failure to detect critical defects during testing, leading to system failures
Category: Operational
RiskType: Inherent
BusinessImpact: Delays in project timelines, increased costs for bug fixes, potential reputational damag
RiskDescription: Failure to develop a comprehensive test plan may result in inadequate testing coverag

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training on test plan development", "2": "Implement peer review process f
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1035:
RiskId: 1685
ComplianceId: 2339
RiskTitle: Late Approval of Test Plan
Criticality: Medium
PossibleDamage: Rushed testing, missed defects, compromised system quality
Category: Operational
RiskType: Inherent
BusinessImpact: Potential rework, compromised system quality, delays in project timelines
RiskDescription: Late approval of the test plan may result in rushed testing, missed defects, and compr
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear approval timelines for test plans", "2": "Implement escalation proce
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1036:
RiskId: 1686

ComplianceId: 2340
RiskTitle: Undetected Defects in System
Criticality: High
PossibleDamage: Quality issues in the final product
Category: Operational
RiskType: Inherent
BusinessImpact: Delays in project delivery and potential rework costs
RiskDescription: Failure to execute testing activities properly may lead to undetected defects in the sys
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review of test execution progress", "2": "Training on proper testing proced
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1037:
RiskId: 1687
ComplianceId: 2341
RiskTitle: Miscommunication Due to Undocumented Test Results
Criticality: Medium
PossibleDamage: Unresolved defects in the system
Category: Operational
RiskType: Inherent
BusinessImpact: Increased time and effort required for defect resolution
RiskDescription: Failure to document test results may lead to miscommunication and unresolved defec
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish clear documentation guidelines", "2": "Regular audit of test result docum
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1038:
RiskId: 1688
ComplianceId: 2342
RiskTitle: Inconsistent Quality Standards
Criticality: High
PossibleDamage: Inconsistent quality may lead to project failures and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential project delays, increased costs, dissatisfied customers
RiskDescription: Failure to document quality attributes may result in inconsistent quality standards, lea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular quality audits", "2": "Training on quality attribute documentation", "3": "Us
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1039:
RiskId: 1689
ComplianceId: 2343
RiskTitle: Subjective Evaluation of Deliverables
Criticality: Medium
PossibleDamage: Subjective evaluations may lead to inconsistent quality assessments and project del

Category: Operational
RiskType: Current
BusinessImpact: Potential project delays, increased costs, quality issues
RiskDescription: Lack of measurable assessment metrics may result in subjective evaluations, leading
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Standardized assessment templates", "2": "Regular reviews of assessment metric
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1040:
RiskId: 1690
ComplianceId: 2344
RiskTitle: Biased Quality Assurance Evaluations
Criticality: High
PossibleDamage: Inaccurate project quality assessments and compromised deliverables
Category: Operational
RiskType: Inherent
BusinessImpact: Potential project delays, rework, and stakeholder dissatisfaction
RiskDescription: The lack of an independent quality assurance team may lead to biased evaluations, in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear guidelines for the independence of the quality assurance team", "2
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1041:
RiskId: 1691
ComplianceId: 2345
RiskTitle: Security Vulnerabilities in Code
Criticality: High
PossibleDamage: Increased risk of security breaches and data leaks
Category: IT
RiskType: Current
BusinessImpact: Potential compromise of sensitive data and loss of customer trust
RiskDescription: Failure to adhere to secure coding standards may result in the introduction of vulnera
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular code reviews", "2": "Training on secure coding practices", "3": "Utilize aut
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1042:
RiskId: 1692
ComplianceId: 2346
RiskTitle: Undetected Security Vulnerabilities
Criticality: Medium
PossibleDamage: Undetected security vulnerabilities leading to potential breaches
Category: IT
RiskType: Current
BusinessImpact: Potential compromise of sensitive data and system integrity
RiskDescription: Failure to conduct regular code reviews may result in undetected vulnerabilities that c

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish code review schedules", "2": "Utilize automated code analysis tools", "3"
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1043:
RiskId: 1693
ComplianceId: 2347
RiskTitle: Deployment of Software with Critical Bugs
Criticality: High
PossibleDamage: Data breaches, system failures, loss of customer trust
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Failure to conduct comprehensive testing may result in critical bugs going undetected
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated testing pipelines", "2": "Establish clear testing criteria and m
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1044:
RiskId: 1694

ComplianceId: 2348
RiskTitle: Inadequate Testing Cycles
Criticality: Medium
PossibleDamage: Post-deployment issues, user dissatisfaction, increased support costs
Category: Operational
RiskType: Current
BusinessImpact: Increased workload for support teams, potential loss of customers
RiskDescription: Insufficient testing cycles may result in software issues going unnoticed until after dep
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement continuous integration and continuous deployment practices", "2": "Est
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1045:
RiskId: 1695
ComplianceId: 2349
RiskTitle: Incomplete Documentation of SDLC Processes
Criticality: High
PossibleDamage: Increased risk of software defects, security vulnerabilities, and compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Delays in project delivery, increased rework, potential legal consequences
RiskDescription: Lack of comprehensive documentation may lead to misunderstandings, errors, and de
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits of documentation completeness and accuracy", "2": "Training sess

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 1046:

RiskId: 1696

ComplianceId: 2350

RiskTitle: Lack of Training for Software Development Personnel

Criticality: Medium

PossibleDamage: Outdated skills, inefficient processes, and increased error rates in software developr

Category: Operational

RiskType: Residual

BusinessImpact: Decreased productivity, quality issues, employee dissatisfaction

RiskDescription: Lack of training may result in outdated skills, inefficient processes, and increased erro

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Develop a training curriculum based on industry standards and best practices", "2

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 1047:

RiskId: 1697

ComplianceId: 2351

RiskTitle: Undetected Vulnerabilities in Source Code

Criticality: High

PossibleDamage: Security breaches, data leaks, reputational damage

Category: IT
RiskType: Residual
BusinessImpact: Disruption of services, loss of sensitive data, financial losses
RiskDescription: Failure to conduct systematic source code reviews may result in undetected vulnerab
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated code review tools", "2": "Establish clear review guidelines",
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1048:
RiskId: 1698
ComplianceId: 2352
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data exposure, financial losses, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Failure to detect and address security vulnerabilities in applications may lead to data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security testing and updates", "2": "Encryption of sensitive data", "3": "Im
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1049:
RiskId: 1699
ComplianceId: 2353
RiskTitle: Post-Update Vulnerability Risk
Criticality: Medium
PossibleDamage: Data exposure, application downtime, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, financial losses
RiskDescription: Failure to conduct security testing post-update may introduce new vulnerabilities and
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish update testing protocols", "2": "Implement version control for updates", "
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1050:
RiskId: 1700
ComplianceId: 2354
RiskTitle: Security Vulnerabilities in Third-Party Software
Criticality: High
PossibleDamage: Security breaches, data leaks, system compromise
Category: IT
RiskType: Residual
BusinessImpact: Disruption of services, loss of sensitive data
RiskDescription: Failure to review and test third-party software can lead to exploitable vulnerabilities ar

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular security assessments and updates", "2": "Enforce strict access
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1051:
RiskId: 1701
ComplianceId: 2355
RiskTitle: Security Vulnerabilities in Software
Criticality: High
PossibleDamage: Data breaches, system vulnerabilities, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Potential compromise of sensitive data and disruption of business operations
RiskDescription: Failure to implement secure coding standards could result in the introduction of secur
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on secure coding practices", "2": "Utilize automated code analysi
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1052:
RiskId: 1702

ComplianceId: 2356
RiskTitle: Insecure Code Deployment
Criticality: Medium
PossibleDamage: System vulnerabilities, potential breaches
Category: Operational
RiskType: Inherent
BusinessImpact: Deployment of insecure code could lead to system vulnerabilities and potential breac
RiskDescription: Failure to conduct source code reviews could result in the deployment of insecure co
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear code review guidelines", "2": "Utilize automated code review tools"
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1053:
RiskId: 1703
ComplianceId: 2357
RiskTitle: Undetected Security Vulnerabilities
Criticality: High
PossibleDamage: Increased risk of security breaches and data loss
Category: Operational
RiskType: Current
BusinessImpact: Development, Operations, Security
RiskDescription: Failure to automate security checks may result in undetected vulnerabilities that can b
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement automated security scanning tools", "2": "Regularly review and update

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1054:

RiskId: 1704

ComplianceId: 2358

RiskTitle: Lack of Security Compliance Metrics

Criticality: Medium

PossibleDamage: Increased risk of non-compliance and security incidents

Category: Operational

RiskType: Current

BusinessImpact: Development, Operations, Security

RiskDescription: Without established metrics for security compliance, there is a higher chance of overl

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement automated security metric tracking tools", "2": "Regularly review and u

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 1055:

RiskId: 1705

ComplianceId: 2359

RiskTitle: Unauthorized Third-Party API Access

Criticality: High

PossibleDamage: Unauthorized access to sensitive data, data breaches, compromised system integrit

Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches, compromised system integrity, and reputational damage.
RiskDescription: Unauthorized third-party API access can lead to data breaches, compromised system
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication and authorization mechanisms for API access", "
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1056:
RiskId: 1706
ComplianceId: 2360
RiskTitle: Insecure API Development Practices
Criticality: High
PossibleDamage: Data breaches, system vulnerabilities, unauthorized access.
Category: IT
RiskType: Current
BusinessImpact: Data breaches, compromised system integrity, and reputational damage.
RiskDescription: Insecure API development practices can lead to data breaches, system vulnerabilities
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Adopt security frameworks such as OWASP API Security Top 10", "2": "Regularly
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1057:
RiskId: 1707
ComplianceId: 2361
RiskTitle: Unauthorized API Access Risk
Criticality: High
PossibleDamage: Data breaches, unauthorized data access, financial losses.
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory fines, damage to reputation.
RiskDescription: Risk of unauthorized third parties gaining access to sensitive data through APIs, leadi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication and authorization mechanisms for API access.",
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1058:
RiskId: 1708
ComplianceId: 2362
RiskTitle: API Security Vulnerability Risk
Criticality: Medium
PossibleDamage: Data breaches, security incidents, regulatory fines.
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, system downtime, regulatory fines.
RiskDescription: Risk of security vulnerabilities in APIs leading to data breaches, system compromise,

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement security patches and updates based on assessment findings.", "2": "R
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1059:
RiskId: 1709
ComplianceId: 2363
RiskTitle: Data Breach Due to Lack of Encryption
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties, legal consequences
RiskDescription: Failure to implement encryption standards may result in unauthorized access to sensi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security audits to ensure encryption standards are being followed", "2": "I
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1060:
RiskId: 1710

ComplianceId: 2364
RiskTitle: Unauthorized Access to APIs
Criticality: Medium
PossibleDamage: Data breaches, misuse of API resources, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial losses, reputational damage
RiskDescription: Failure to monitor API usage may result in unauthorized access, leading to data brea
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing real-time alerts for unusual API usage patterns", "2": "Regularly rev
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1061:
RiskId: 1711
ComplianceId: 2365
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, compromise of system integrity, reputational
Category: Operational
RiskType: Residual
BusinessImpact: Potential data breaches, legal implications, reputational harm
RiskDescription: Risk of unauthorized access by third parties due to inadequate vetting process, leadi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strong access controls and monitoring mechanisms", "2": "Regularly u

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1062:

RiskId: 1712

ComplianceId: 2366

RiskTitle: Data Breach due to API Vulnerabilities

Criticality: High

PossibleDamage: Financial losses, reputational damage, legal implications

Category: IT

RiskType: Inherent

BusinessImpact: Loss of sensitive data, regulatory fines, damage to reputation

RiskDescription: Failure to conduct risk assessments may lead to vulnerabilities in APIs that can be ex

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement API security best practices", "2": "Regularly update API security measu

CreatedAt: 2025-10-27 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 1063:

RiskId: 1713

ComplianceId: 2367

RiskTitle: Data Breach due to Lack of Encryption

Criticality: High

PossibleDamage: Loss of sensitive data, financial penalties, reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, legal consequences
RiskDescription: Failure to implement encryption could lead to unauthorized access to sensitive data tr
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption protocols", "2": "Regularly update encryption keys", "3": "Mo
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1064:
RiskId: 1714
ComplianceId: 2368
RiskTitle: Unauthorized Access due to Expired Tokens
Criticality: Medium
PossibleDamage: Data breaches, unauthorized system access, misuse of API tokens
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, reputational damage, legal consequences
RiskDescription: Failure to enforce token expiration policies could lead to unauthorized access and mis
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement token expiration policies", "2": "Monitor token usage", "3": "Enforce tok
CreatedAt: 2025-10-27 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1065:
RiskId: 1317
ComplianceId: 1969
RiskTitle: Non-Compliance with Bi-Annual Self-Assessment Requirement
Criticality: High
PossibleDamage: Regulatory penalties and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: All regulatory agencies
RiskDescription: Failure to conduct bi-annual self-assessments may lead to non-compliance with MFR
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust self-assessment process", "2": "Regular training for complianc
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1066:
RiskId: 1318
ComplianceId: 1970
RiskTitle: Lack of Training Risk
Criticality: High
PossibleDamage: Increased risk of food safety incidents due to lack of knowledge
Category: Operational
RiskType: Inherent
BusinessImpact: Potential contamination of food products and health hazards
RiskDescription: Personnel not adequately trained may overlook critical food safety procedures, leadin

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training completion status", "2": "Providing additional suppo
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1067:
RiskId: 1319
ComplianceId: 1971
RiskTitle: Non-Compliance with Bi-Annual Inspection Requirement
Criticality: High
PossibleDamage: Risk of food safety hazards and regulatory penalties
Category: Operational
RiskType: Current
BusinessImpact: Potential harm to consumers, regulatory fines
RiskDescription: Failure to conduct bi-annual inspections may result in undetected safety hazards and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training programs for facility staff on food safety standards", "2
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1068:
RiskId: 1320

ComplianceId: 1972
RiskTitle: Inaccurate Documentation of Inspection Results
Criticality: Medium
PossibleDamage: Risk of non-compliance issues going unnoticed
Category: Operational
RiskType: Current
BusinessImpact: Potential regulatory violations, compromised food safety
RiskDescription: Failure to accurately document inspection results may lead to oversight of non-compli
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement standardized reporting templates for inspection results", "2": "Establish
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1069:
RiskId: 1321
ComplianceId: 1973
RiskTitle: Communication Breakdown
Criticality: High
PossibleDamage: Delayed response to food safety issues and potential outbreaks
Category: Operational
RiskType: Current
BusinessImpact: Regulatory compliance compromised, public health at risk
RiskDescription: Lack of effective communication channels may result in delays in addressing food saf
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear communication protocols and escalation procedures", "2": "Implem

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 1070:

RiskId: 1322

ComplianceId: 1974

RiskTitle: Lack of Documented Meeting Minutes

Criticality: Medium

PossibleDamage: Disputes over decisions, lack of accountability, miscommunication

Category: Operational

RiskType: Current

BusinessImpact: Decision-making process compromised, lack of transparency

RiskDescription: Failure to document meeting minutes may result in disputes over decisions, lack of ac

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Designate a meeting secretary responsible for accurate documentation", "2": "Imp

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 1071:

RiskId: 1323

ComplianceId: 1975

RiskTitle: Miscommunication due to Outdated Definitions

Criticality: High

PossibleDamage: Incorrect decisions, regulatory non-compliance, operational inefficiencies

Category: Operational
RiskType: Inherent
BusinessImpact: Impacts all areas of the organization relying on accurate definitions.
RiskDescription: Outdated definitions can lead to misunderstandings, errors, and inefficiencies in opera
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on updated definitions", "2": "Automated alerts for review deadlin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1072:
RiskId: 1324
ComplianceId: 1976
RiskTitle: Misinterpretation of Key Terms
Criticality: High
PossibleDamage: Non-compliance with regulations, increased risk of food safety incidents
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential regulatory fines, reputation damage, and compromised food safety
RiskDescription: Failure to understand key terms may lead to incorrect application of regulations and p
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide refresher training sessions for employees who struggle with understandin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1073:
RiskId: 1325
ComplianceId: 1977
RiskTitle: Inadequate Basic Training for Inspectors
Criticality: High
PossibleDamage: Increased risk of missing critical food safety violations
Category: Operational
RiskType: Inherent
BusinessImpact: Potential for foodborne illness outbreaks or product recalls
RiskDescription: Insufficient basic training may lead inspectors to overlook key food safety issues, resu
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide additional on-the-job training for inspectors who have not completed the b
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1074:
RiskId: 1326
ComplianceId: 1978
RiskTitle: Lack of Field Training for Inspectors
Criticality: High
PossibleDamage: Inadequate practical skills to identify and address food safety risks
Category: Operational
RiskType: Inherent
BusinessImpact: Increased likelihood of undetected food safety violations
RiskDescription: Inspectors without field training may struggle to apply theoretical knowledge to real-w

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 60
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Assign experienced mentors to guide inspectors during field training", "2": "Provid
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1075:
RiskId: 1327
ComplianceId: 1979
RiskTitle: Inadequate Trainer Competency
Criticality: High
PossibleDamage: Compromised food safety standards and potential incidents
Category: Operational
RiskType: Inherent
BusinessImpact: Decreased effectiveness of the food safety program and potential legal implications.
RiskDescription: Trainers lacking competency may provide inaccurate information during training sessi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a standardized competency assessment process", "2": "Provide additi
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1076:
RiskId: 1328

ComplianceId: 1980
RiskTitle: Unapproved Trainer Conducting Sessions
Criticality: Medium
PossibleDamage: Compromised food safety standards and potential incidents
Category: Operational
RiskType: Inherent
BusinessImpact: Decreased effectiveness of the food safety program and potential legal implications.
RiskDescription: Trainers conducting sessions without proper approval may lack necessary qualificatio
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear approval criteria for trainers", "2": "Provide training for the Food Sa
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1077:
RiskId: 1329
ComplianceId: 1981
RiskTitle: Non-compliance due to lack of updated audit training
Criticality: High
PossibleDamage: Inaccurate audit assessments and potential violations of food safety standards
Category: Operational
RiskType: Current
BusinessImpact: Potential fines, legal actions, and reputational damage
RiskDescription: Auditors may overlook critical compliance issues or fail to identify non-conformities du
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly update audit training materials to reflect current standards and regulatio
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1078:
RiskId: 1330
ComplianceId: 1982
RiskTitle: Non-compliance due to lack of verification audit participation
Criticality: Medium
PossibleDamage: Inadequate validation of audit skills and potential oversight of critical compliance issu
Category: Operational
RiskType: Current
BusinessImpact: Potential non-conformities, regulatory violations, and compromised food safety
RiskDescription: Auditors may lack practical experience in conducting audits effectively, leading to pote
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide hands-on training opportunities for auditors to practice audit skills", "2": "E
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1079:
RiskId: 1331
ComplianceId: 1983
RiskTitle: Outdated Procedure for Evaluation of Legal Authority
Criticality: High
PossibleDamage: Legal fines, regulatory penalties, reputational damage

Category: Compliance
RiskType: Current
BusinessImpact: Increased legal and regulatory scrutiny, financial penalties
RiskDescription: Failure to update the written procedure for evaluating legal authority may result in usi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular legal updates and training for compliance officer", "2": "Establishing a leg
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1080:
RiskId: 1332
ComplianceId: 1984
RiskTitle: Inadequate Documentation of Legal Authority Assessments
Criticality: Medium
PossibleDamage: Challenges in proving compliance, regulatory fines, legal disputes
Category: Compliance
RiskType: Current
BusinessImpact: Increased scrutiny during audits, potential legal disputes
RiskDescription: Failure to document legal authority assessments may lead to difficulties in demonstra
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing standardized documentation practices", "2": "Regular review and ve
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1081:
RiskId: 1333
ComplianceId: 1985
RiskTitle: Regulatory Penalties and Legal Challenges
Criticality: High
PossibleDamage: Non-compliance consequences
Category: Compliance
RiskType: Current
BusinessImpact: State program operations and reputation at risk
RiskDescription: Failure to comply with regulatory equivalency assessments may lead to penalties and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Review findings with legal counsel", "2": "Implement necessary changes based or
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1082:
RiskId: 1334
ComplianceId: 1986
RiskTitle: Lack of Completion of Basic Food Inspection Training Curriculum
Criticality: High
PossibleDamage: Potential health hazards, regulatory violations, and compromised food safety
Category: Operational
RiskType: Inherent
BusinessImpact: Inspector Training Department may face increased scrutiny, fines, and reputational da
RiskDescription: Inspectors lacking essential training may overlook critical food safety violations, leadi

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of inspector training progress", "2": "Providing additional supp
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1083:
RiskId: 1335
ComplianceId: 1987
RiskTitle: Inadequate Delivery of Basic Food Inspection Training
Criticality: Medium
PossibleDamage: Ineffective inspections, public health risks, and potential legal liabilities
Category: Operational
RiskType: Inherent
BusinessImpact: Training Department may face increased training costs, legal disputes, and reputation
RiskDescription: Insufficient training delivery methods may result in inspectors lacking essential knowle
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular evaluation of training effectiveness", "2": "Feedback mechanisms for con
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1084:
RiskId: 1336

ComplianceId: 1988
RiskTitle: Inadequate Training Leading to Incorrect Inspections
Criticality: High
PossibleDamage: Increased risk of foodborne illness outbreaks and damage to public trust
Category: Operational
RiskType: Current
BusinessImpact: Potential harm to consumers and reputation damage
RiskDescription: Inspectors conducting specialized inspections without proper training may overlook cr
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of inspector training progress", "2": "Providing additional supp
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1085:
RiskId: 1337
ComplianceId: 1989
RiskTitle: Insufficient Field Training Leading to Inadequate Inspections
Criticality: Medium
PossibleDamage: Increased risk of regulatory non-compliance and potential fines
Category: Operational
RiskType: Current
BusinessImpact: Risk of regulatory penalties and damage to department reputation
RiskDescription: Inspectors conducting independent specialized inspections without proper field trainin
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Scheduling regular joint field training sessions", "2": "Providing feedback and guid
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1086:
RiskId: 1338
ComplianceId: 1990
RiskTitle: Non-compliance due to incomplete documentation
Criticality: High
PossibleDamage: Non-compliance penalties, loss of credibility
Category: Compliance
RiskType: Current
BusinessImpact: Disruption of operations, financial penalties
RiskDescription: Failure to document training records accurately may result in non-compliance with reg
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of training records for accuracy", "2": "Training on proper documen
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1087:
RiskId: 1339
ComplianceId: 1991
RiskTitle: Non-compliance due to inadequate record retention
Criticality: Medium
PossibleDamage: Non-compliance penalties, regulatory scrutiny

Category: Compliance
RiskType: Current
BusinessImpact: Potential penalties, reputational damage
RiskDescription: Failure to retain training records for inactive inspectors may result in non-compliance
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review of retention policies to ensure compliance", "2": "Automated remin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1088:
RiskId: 1340
ComplianceId: 1992
RiskTitle: Lack of Continuing Education Compliance
Criticality: High
PossibleDamage: Increased risk of inspection errors and compromised food safety
Category: Operational
RiskType: Current
BusinessImpact: Potential foodborne illness outbreaks, product recalls, and damage to the program's r
RiskDescription: Failure to comply with continuing education requirements may result in inspectors lac
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly communicate the importance of continuing education to inspectors and
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 1089:
RiskId: 1341
ComplianceId: 1993
RiskTitle: Non-Submission of Continuing Education Documentation
Criticality: High
PossibleDamage: Non-compliance with regulatory requirements, potential suspension of inspection pri
Category: Compliance
RiskType: Inherent
BusinessImpact: Disruption to inspection activities, financial penalties, reputational damage
RiskDescription: Failure to submit required documentation for continuing education activities within the
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reminders to inspectors about documentation deadlines", "2": "Training o
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1090:
RiskId: 1342
ComplianceId: 1994
RiskTitle: Unverified Training Approval
Criticality: High
PossibleDamage: Misinformation and non-compliance due to inadequate training sources
Category: Operational
RiskType: Current
BusinessImpact: Potential violations of regulations and compromised inspection quality
RiskDescription: Inspectors attending training from unapproved sources may not receive accurate or u

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update the list of approved training sources", "2": "Provide ongoing trair
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1091:
RiskId: 1343
ComplianceId: 1995
RiskTitle: Missed Training Deadline
Criticality: Medium
PossibleDamage: Non-compliance and potential penalties due to missed training deadlines
Category: Operational
RiskType: Current
BusinessImpact: Potential penalties and reputation damage
RiskDescription: Inspectors failing to complete training within the designated timeframe may lead to no
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated reminders for upcoming training deadlines", "2": "Provide ir
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1092:
RiskId: 1344

ComplianceId: 1996
RiskTitle: Inaccurate Risk Classification
Criticality: High
PossibleDamage: Increased risk of foodborne illnesses and regulatory violations
Category: Operational
RiskType: Inherent
BusinessImpact: Potential harm to public health and reputation of the State program
RiskDescription: Incorrect risk classification may lead to inadequate inspection frequency for high-risk
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of risk categories", "2": "Training programs for accurat
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1093:
RiskId: 1345
ComplianceId: 1997
RiskTitle: Missed Operational Changes
Criticality: Medium
PossibleDamage: Increased risk of non-compliance and food safety incidents
Category: Operational
RiskType: Inherent
BusinessImpact: Potential regulatory fines and public health risks
RiskDescription: Failure to conduct timely risk assessments may result in missed operational changes
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Automated alerts for operational changes", "2": "Regular communication channels

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1094:

RiskId: 1346

ComplianceId: 1998

RiskTitle: Incomplete Inspection Reports

Criticality: High

PossibleDamage: Undetected violations or risks

Category: Operational

RiskType: Inherent

BusinessImpact: Potential harm to consumers and damage to the state's reputation

RiskDescription: Failure to conduct thorough inspections may result in critical violations going unnotice

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Provide thorough training on inspection procedures", "2": "Implement quality contr

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 1095:

RiskId: 1347

ComplianceId: 1999

RiskTitle: Failure to Prioritize High-Risk Establishments

Criticality: Medium

PossibleDamage: Critical violations going undetected

Category: Operational
RiskType: Inherent
BusinessImpact: Potential harm to consumers and damage to the state's reputation
RiskDescription: Failure to prioritize high-risk establishments may result in critical violations going unde
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly assess and update risk assessment criteria", "2": "Implement a system
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1096:
RiskId: 1348
ComplianceId: 2000
RiskTitle: Delayed Consumer Complaint Response
Criticality: High
PossibleDamage: Delayed response to consumer complaints leading to dissatisfaction and potential le
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of consumer trust, potential legal consequences
RiskDescription: Failure to log and acknowledge consumer complaints within 24 hours may result in de
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated logging and acknowledgment system", "2": "Provide regula
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1097:
RiskId: 1349
ComplianceId: 2001
RiskTitle: Ineffective Complaint Tracking
Criticality: Medium
PossibleDamage: Ineffective tracking leading to delayed or missed responses to consumer complaints
Category: Operational
RiskType: Inherent
BusinessImpact: Increased consumer dissatisfaction, potential legal consequences
RiskDescription: Failure to utilize an effective tracking system for consumer complaints may result in d
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a centralized tracking system for all complaints", "2": "Regularly review
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1098:
RiskId: 1350
ComplianceId: 2002
RiskTitle: Failure to Follow Written Recall Procedures
Criticality: High
PossibleDamage: Consumer health risks, regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential harm to consumers, financial penalties, loss of consumer trust
RiskDescription: Not having established written recall procedures may lead to delays in identifying safe

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of procedures", "2": "Training for staff on recall protoc
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1099:
RiskId: 1351
ComplianceId: 2003
RiskTitle: Delayed Initiation of Recalls
Criticality: High
PossibleDamage: Increased health risks for consumers, regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential harm to consumers, financial penalties, loss of consumer trust
RiskDescription: Delaying the initiation of recalls upon identifying safety issues can lead to increased h
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear escalation procedures for safety issues", "2": "Regular training on
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1100:
RiskId: 1352

ComplianceId: 2004
RiskTitle: Inadequate Public Health Monitoring
Criticality: High
PossibleDamage: Compromised public health data accuracy
Category: Compliance
RiskType: Current
BusinessImpact: Loss of public trust, potential health risks due to inaccurate data
RiskDescription: Failure to provide accurate public health data due to lack of oversight in the absence
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure alternative measures are effective", "2": "Engage externa
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1101:
RiskId: 1353
ComplianceId: 2005
RiskTitle: Loss of Inspection Data
Criticality: High
PossibleDamage: Loss of critical inspection data may lead to regulatory non-compliance and operation
Category: Compliance
RiskType: Current
BusinessImpact: Non-compliance with record retention requirements may result in fines, legal actions,
RiskDescription: Failure to retain inspection reports may hinder the ability to address compliance issue
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure all inspection reports are properly retained", "2": "Trainin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1102:
RiskId: 1354
ComplianceId: 2006
RiskTitle: Unresolved Consumer Complaints
Criticality: Medium
PossibleDamage: Failure to address consumer complaints effectively may result in product recalls, neg
Category: Compliance
RiskType: Current
BusinessImpact: Unresolved consumer complaints can lead to reputational damage, decreased consu
RiskDescription: Inadequate retention of consumer complaints may hinder the ability to identify and ad
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing a standardized process for documenting and tracking consumer co
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1103:
RiskId: 1355
ComplianceId: 2007
RiskTitle: Insufficient Audit Frequency
Criticality: High
PossibleDamage: Overlooked violations and safety hazards going undetected

Category: Compliance
RiskType: Inherent
BusinessImpact: Potential compromise of safety standards and regulatory compliance
RiskDescription: Inadequate audit frequency increases the likelihood of missing critical issues during in
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust audit scheduling system to track and ensure timely audits", "2
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1104:
RiskId: 1356
ComplianceId: 2008
RiskTitle: Inadequate Documentation of Audit Findings
Criticality: Medium
PossibleDamage: Misinterpretation of findings or lack of evidence for corrective actions
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential delays in addressing compliance issues and implementing corrective actions
RiskDescription: Incomplete or inaccurate documentation of audit findings may lead to misunderstandi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide training on proper documentation procedures to all inspectors", "2": "Impl
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1105:
RiskId: 1357
ComplianceId: 2009
RiskTitle: Inaccurate Inspection Reporting
Criticality: High
PossibleDamage: Incorrect decisions based on faulty reports
Category: Operational
RiskType: Current
BusinessImpact: Quality of decision-making processes affected
RiskDescription: Failure to accurately report inspection findings could lead to incorrect decisions and a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training sessions for staff on reporting standards", "2": "Implem
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1106:
RiskId: 1358
ComplianceId: 2010
RiskTitle: Inaccurate Sample Reporting
Criticality: High
PossibleDamage: Legal penalties and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential legal consequences and damage to organizational reputation
RiskDescription: Non-compliance with sample report audit procedures may lead to inaccurate sample r

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training sessions for Quality Assurance staff on sample collecti
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1107:
RiskId: 1359
ComplianceId: 2011
RiskTitle: Inaccurate Evaluation of Sample Reports
Criticality: Medium
PossibleDamage: Incorrect conclusions and decisions
Category: Operational
RiskType: Current
BusinessImpact: Potential impact on decision-making processes and quality of evaluation
RiskDescription: Non-compliance with performance factor evaluation may lead to inaccurate evaluation
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update and align performance factors with industry standards", "2": "Imp
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1108:
RiskId: 1360

ComplianceId: 2012
RiskTitle: Failure to Implement Corrective Action Plan
Criticality: High
PossibleDamage: Continued poor performance, decreased quality, potential non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Decreased quality, potential non-compliance, operational inefficiencies
RiskDescription: Failure to implement corrective actions may result in ongoing performance issues, rec
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide immediate training and support to improve performance", "2": "Implement
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1109:
RiskId: 1361
ComplianceId: 2013
RiskTitle: Lack of Coordination with State Agencies
Criticality: High
PossibleDamage: Delayed or ineffective response to food-related incidents
Category: Operational
RiskType: Inherent
BusinessImpact: Potential impact on public health and safety
RiskDescription: Failure to establish a memorandum of understanding with state agencies may result i
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly review and update the memorandum of understanding", "2": "Conduct j

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1110:

RiskId: 1362

ComplianceId: 2014

RiskTitle: Lack of Designated Response Coordinators

Criticality: Medium

PossibleDamage: Confusion and delays in response coordination during food-related incidents

Category: Operational

RiskType: Inherent

BusinessImpact: Potential impact on response timeliness and effectiveness

RiskDescription: Failure to designate response coordinators may result in unclear responsibilities, com

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Provide training and resources to designated response coordinators", "2": "Establ

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 1111:

RiskId: 1363

ComplianceId: 2015

RiskTitle: Delayed Response to Outbreaks

Criticality: High

PossibleDamage: Increased illnesses, potential legal liabilities

Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, public health concerns
RiskDescription: Failure to maintain accurate logs may result in delayed response to outbreaks, leadin
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on log maintenance procedures", "2": "Automated alerts for incor
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1112:
RiskId: 1364
ComplianceId: 2016
RiskTitle: Missed Opportunities for Outbreak Prevention
Criticality: Medium
PossibleDamage: Increased risk of outbreaks and public health concerns
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, public health concerns
RiskDescription: Failure to utilize epidemiological data effectively may result in missed opportunities to
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on data analysis techniques", "2": "Cross-functional collaboration
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1113:
RiskId: 1365
ComplianceId: 2017
RiskTitle: Inadequate Investigation Risk
Criticality: High
PossibleDamage: Potential consumer illnesses, product recalls, regulatory fines, and reputational dam
Category: Operational
RiskType: Inherent
BusinessImpact: Significant financial losses, legal liabilities, and damage to brand reputation.
RiskDescription: Failure to conduct thorough investigations may result in the failure to identify and add
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement standardized investigation protocols", "2": "Provide continuous training
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1114:
RiskId: 1366
ComplianceId: 2018
RiskTitle: Misinformation on Food-Related Hazards
Criticality: High
PossibleDamage: Misinformation leading to incorrect public response to food-related incidents, potenti
Category: Operational
RiskType: Current
BusinessImpact: Public health and communication departments would face reputational damage and l
RiskDescription: Incorrect information dissemination could lead to panic among the public and increase

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure information accuracy through verification processes", "2": "Regularly upda
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1115:
RiskId: 1367
ComplianceId: 2019
RiskTitle: Inconsistent Media Communications
Criticality: Medium
PossibleDamage: Inconsistent or delayed communication leading to public confusion, mistrust, and po
Category: Operational
RiskType: Current
BusinessImpact: Public health and communication departments may face public backlash and reputati
RiskDescription: Delayed or inconsistent communication could result in public confusion, mistrust, and
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication protocols and chains of command", "2": "Conduct
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1116:
RiskId: 1368

ComplianceId: 2020
RiskTitle: Incomplete Reporting to Relevant Agencies
Criticality: High
PossibleDamage: Legal or regulatory consequences due to incomplete reporting
Category: Operational
RiskType: Current
BusinessImpact: Potential fines, penalties, or reputational damage
RiskDescription: Failure to maintain comprehensive records may result in incomplete or inaccurate rep
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on proper documentation procedures", "2": "Implement
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1117:
RiskId: 1369
ComplianceId: 2021
RiskTitle: Delayed Response by Relevant Agencies
Criticality: High
PossibleDamage: Public health and safety impact due to delayed response
Category: Operational
RiskType: Current
BusinessImpact: Potential public outcry, legal liabilities, or reputational damage
RiskDescription: Failure to distribute final reports timely may result in delayed response or inadequate
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 63.51
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear communication protocols with relevant agencies", "2": "Implement
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1118:
RiskId: 1370
ComplianceId: 2022
RiskTitle: Undetected Critical Violations
Criticality: High
PossibleDamage: Legal actions, financial penalties, and reputational damage.
Category: Compliance
RiskType: Current
BusinessImpact: All business units within the State agency and relevant third-party vendors.
RiskDescription: Failure to detect critical violations may lead to legal consequences, financial penalties
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for compliance officers and staff on monitoring procedu
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1119:
RiskId: 1371
ComplianceId: 2023
RiskTitle: Failure to Conduct Annual Performance Reviews
Criticality: High
PossibleDamage: Unidentified compliance issues and lack of improvement

Category: Compliance
RiskType: Current
BusinessImpact: Impact on compliance program effectiveness and reputation
RiskDescription: Failure to conduct annual performance reviews may result in overlooked compliance i
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear guidelines for conducting reviews", "2": "Provide training on perform
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1120:
RiskId: 1372
ComplianceId: 2024
RiskTitle: Incomplete Documentation of Outreach Activities
Criticality: High
PossibleDamage: Inaccurate evaluation of outreach efforts and hindered improvement opportunities
Category: Operational
RiskType: Residual
BusinessImpact: State program's ability to effectively engage with the community and achieve outreach
RiskDescription: Failure to document outreach activities accurately and timely may result in ineffective
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training sessions for personnel on proper documentation proce
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1121:
RiskId: 1373
ComplianceId: 2025
RiskTitle: Ineffective Evaluation of Outreach Activities
Criticality: Medium
PossibleDamage: Continuation of ineffective outreach strategies and missed improvement opportunitie
Category: Operational
RiskType: Residual
BusinessImpact: State program's ability to effectively engage with the community and achieve outreach
RiskDescription: Failure to evaluate outreach activities effectively may lead to the perpetuation of ineffe
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear evaluation criteria and metrics for consistency", "2": "Implement re
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1122:
RiskId: 1374
ComplianceId: 2026
RiskTitle: Inadequate Resource Allocation
Criticality: High
PossibleDamage: Operational inefficiencies and non-compliance
Category: Operational
RiskType: Current
BusinessImpact: State program management team and program delivery
RiskDescription: Failure to adequately assess and allocate resources may result in staffing shortages,

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on resource assessment procedures", "2": "Implement automate
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1123:
RiskId: 1375
ComplianceId: 2027
RiskTitle: Resource Misalignment with Program Requirements
Criticality: Medium
PossibleDamage: Non-compliance and operational inefficiencies
Category: Operational
RiskType: Current
BusinessImpact: State program management team and program delivery
RiskDescription: Failure to align resources with changing program requirements may lead to inefficienc
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels for requirement changes", "2": "Impleme
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1124:
RiskId: 1376

ComplianceId: 2028
RiskTitle: Understaffing for Critical Inspections
Criticality: High
PossibleDamage: Missed critical inspections and potential risks to public health
Category: Operational
RiskType: Current
BusinessImpact: Disruption of inspection schedules and potential regulatory non-compliance
RiskDescription: Inadequate staffing levels may result in missed critical inspections, leading to potentia
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review of staffing calculations", "2": "Cross-training of inspectors for flexib
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1125:
RiskId: 1377
ComplianceId: 2029
RiskTitle: Inaccurate Staffing Levels
Criticality: Medium
PossibleDamage: Inefficiencies in inspection processes and potential risks to public health
Category: Operational
RiskType: Current
BusinessImpact: Inefficient allocation of resources and potential regulatory non-compliance
RiskDescription: Failure to adjust staffing levels may result in inefficiencies in inspection processes, lea
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regular review of inspection frequency changes", "2": "Flexible staffing arrangem
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1126:
RiskId: 1378
ComplianceId: 2030
RiskTitle: Inadequate Equipment Inventory
Criticality: High
PossibleDamage: Delays in inspections and sample collections, compromised data quality
Category: Operational
RiskType: Current
BusinessImpact: Disruption of program operations, potential regulatory fines
RiskDescription: Failure to maintain an updated equipment inventory may result in delays and inefficie
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on equipment handling and maintenance", "2": "Establish
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1127:
RiskId: 1379
ComplianceId: 2031
RiskTitle: Delayed Equipment Procurement
Criticality: Medium
PossibleDamage: Equipment shortages during critical operations, compromised data quality

Category: Operational
RiskType: Current
BusinessImpact: Disruption of program operations, potential delays in inspections
RiskDescription: Failure to procure necessary equipment in a timely manner may result in shortages du
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish vendor partnerships for expedited procurement", "2": "Maintain buffer st
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1128:
RiskId: 1380
ComplianceId: 2032
RiskTitle: Baseline Self-Assessment Conduct Risk
Criticality: High
PossibleDamage: Failure to conduct baseline self-assessment may result in unidentified deficiencies a
Category: Compliance
RiskType: Inherent
BusinessImpact: Assessment teams and program managers responsible for conducting assessments a
RiskDescription: Failure to conduct baseline self-assessment may lead to non-compliance with regulat
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure designated appendices and worksheets are utilized accurately", "2": "Reg
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1129:
RiskId: 1381
ComplianceId: 2033
RiskTitle: Strategic Improvement Plan Development Risk
Criticality: Medium
PossibleDamage: Lack of improvement plans may lead to persistent program deficiencies and non-co
Category: Compliance
RiskType: Inherent
BusinessImpact: Assessment teams and program managers responsible for conducting assessments
RiskDescription: Failure to develop a Strategic Improvement Plan may result in unresolved deficiencie
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Prioritize deficiencies based on impact severity", "2": "Allocate resources effective
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1130:
RiskId: 1382
ComplianceId: 2034
RiskTitle: Non-compliance due to outdated documentation
Criticality: High
PossibleDamage: Risk of regulatory fines and penalties, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential regulatory consequences and loss of credibility
RiskDescription: Failure to review documentation annually may result in using outdated procedures or

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear review schedule and assign responsibilities", "2": "Implement a v
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1131:
RiskId: 1383
ComplianceId: 2035
RiskTitle: Document version control issues
Criticality: Medium
PossibleDamage: Risk of using outdated or incorrect documentation
Category: Operational
RiskType: Current
BusinessImpact: Potential errors in program implementation and compliance
RiskDescription: Without a centralized document management system, there is a risk of using outdate
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement access controls to prevent unauthorized changes", "2": "Regularly bac
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1132:
RiskId: 1384

ComplianceId: 2036
RiskTitle: Inaccurate Sample Analysis
Criticality: High
PossibleDamage: Incorrect sample analysis results impacting decision-making and potentially causing
Category: Operational
RiskType: Inherent
BusinessImpact: Potential legal implications, health risks, and environmental harm
RiskDescription: Using non-accredited laboratories may lead to inaccurate sample analysis results, imp
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly verify laboratory accreditation status", "2": "Establish a backup plan in c
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1133:
RiskId: 1385
ComplianceId: 2037
RiskTitle: Risk of Incorrect Test Results
Criticality: High
PossibleDamage: Inaccurate test results impacting decision-making and potentially causing harm
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of credibility, legal implications, potential harm to individuals
RiskDescription: Failure to implement a quality system may lead to errors in testing procedures, resulti
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training and education on quality system requirements", "2": "Internal aud

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 1134:

RiskId: 1386

ComplianceId: 2038

RiskTitle: Incomplete Contract Documentation

Criticality: High

PossibleDamage: Disputes, non-compliance, financial losses

Category: Operational

RiskType: Current

BusinessImpact: Operational disruptions, financial liabilities

RiskDescription: Failure to maintain complete contract documentation may lead to disputes with servic

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly review and update contract documentation", "2": "Implement access co

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 1135:

RiskId: 1387

ComplianceId: 2039

RiskTitle: Outdated Quality Manuals

Criticality: Medium

PossibleDamage: Errors, non-compliance, compromised quality

Category: Operational
RiskType: Current
BusinessImpact: Service errors, regulatory violations
RiskDescription: Failure to maintain updated quality manuals may result in errors in laboratory process
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a documented process for updating quality manuals", "2": "Provide train
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1136:
RiskId: 1388
ComplianceId: 2040
RiskTitle: Non-compliance with Annual Self-Assessment Procedure
Criticality: High
PossibleDamage: Legal penalties, fines, and reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Legal consequences and financial losses
RiskDescription: Failure to conduct annual self-assessment may result in unknowingly violating federal
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on updated regulations", "2": "Internal audits to monitor complian
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1137:
RiskId: 1389
ComplianceId: 2041
RiskTitle: Non-compliance with Bi-annual Training Sessions
Criticality: High
PossibleDamage: Increased risk of food safety violations and regulatory fines
Category: Compliance
RiskType: Current
BusinessImpact: All business units may be impacted by regulatory fines and reputational damage.
RiskDescription: Failure to attend bi-annual training sessions may result in gaps in knowledge of food s
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of regulatory changes", "2": "Providing access to online trainin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1138:
RiskId: 1390
ComplianceId: 2042
RiskTitle: Outdated Training Plan
Criticality: High
PossibleDamage: Inadequately trained inspectors may overlook critical issues during inspections, lead
Category: Operational
RiskType: Inherent
BusinessImpact: Increased risk of compliance violations and compromised inspection quality
RiskDescription: The risk of using outdated training materials and schedules can result in inspectors la

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of training materials", "2": "Continuous monitoring of ir
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1139:
RiskId: 1391
ComplianceId: 2043
RiskTitle: Outdated Training Plan Due to Lack of Annual Review
Criticality: Medium
PossibleDamage: Inspectors may not be aware of the latest regulations and procedures, leading to err
Category: Operational
RiskType: Inherent
BusinessImpact: Increased risk of non-compliance and compromised inspection quality
RiskDescription: Without annual review and updates, the training plan may not reflect the current regul
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a clear timeline for annual review and update", "2": "Engage inspectors
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1140:
RiskId: 1392

ComplianceId: 2044
RiskTitle: Inadequate Inspector Training
Criticality: High
PossibleDamage: Increased risk of missed violations or errors in inspection reports, potentially leading
Category: Operational
RiskType: Inherent
BusinessImpact: Inspector Training Department
RiskDescription: Inspectors may lack the necessary skills and knowledge to conduct thorough food ins
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training completion status", "2": "Providing additional suppo
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1141:
RiskId: 1393
ComplianceId: 2045
RiskTitle: Inadequate Training for Specialized Inspectors
Criticality: High
PossibleDamage: Inaccurate food safety assessments, potential health risks
Category: Operational
RiskType: Current
BusinessImpact: Potential health risks due to inaccurate food safety assessments
RiskDescription: Inspectors lacking essential training may misinterpret inspection results, leading to ina
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Provide additional training sessions for inspectors who have not completed the co

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 1142:

RiskId: 1394

ComplianceId: 2046

RiskTitle: Lack of Practical Experience from Joint Field Training

Criticality: Medium

PossibleDamage: Errors in inspection processes, inaccurate assessments

Category: Operational

RiskType: Current

BusinessImpact: Inaccurate assessments and potential errors in inspection processes

RiskDescription: Inspectors lacking practical experience from joint field training may struggle to apply t

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Schedule regular joint field training sessions with qualified trainers", "2": "Provide

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 1143:

RiskId: 1395

ComplianceId: 2047

RiskTitle: Insufficient Continuing Education

Criticality: High

PossibleDamage: Lack of updated knowledge and skills in inspectors

Category: Operational
RiskType: Inherent
BusinessImpact: Potential errors in inspections and compromised food safety
RiskDescription: Failure to meet the continuing education requirement may result in inspectors lacking
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide access to approved continuing education sources", "2": "Send reminders
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1144:
RiskId: 1396
ComplianceId: 2048
RiskTitle: Non-compliance with Training Record Documentation
Criticality: High
PossibleDamage: Legal penalties, loss of certification, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: HR department's efficiency and inspectors' credibility at risk
RiskDescription: Failure to document training records may lead to regulatory violations, audits, or inspe
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of training records to ensure compliance", "2": "Training sessions f
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1145:
RiskId: 1397
ComplianceId: 2049
RiskTitle: Outdated Knowledge and Skills
Criticality: High
PossibleDamage: Impact on inspection quality and accuracy
Category: Operational
RiskType: Inherent
BusinessImpact: Potential errors in inspections and reduced credibility of inspection reports
RiskDescription: Inspectors lacking up-to-date knowledge and skills may miss critical details during ins
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly communicate the importance of continuing education to inspectors", "2'
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1146:
RiskId: 1398
ComplianceId: 2050
RiskTitle: Lack of Completion of Basic Food Inspection Curriculum Coursework
Criticality: High
PossibleDamage: Inspectors lacking essential knowledge may overlook critical food safety violations d
Category: Operational
RiskType: Inherent
BusinessImpact: Potential health risks for consumers due to missed food safety violations.
RiskDescription: Inspectors may not be able to effectively identify and address food safety violations if

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide additional training sessions for inspectors who have not completed the co
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1147:
RiskId: 1399
ComplianceId: 2051
RiskTitle: Failure to Conduct Annual Field Inspections
Criticality: High
PossibleDamage: Inspectors lacking practical experience may struggle to identify emerging food safety
Category: Operational
RiskType: Inherent
BusinessImpact: Potential health hazards for consumers due to missed food safety risks.
RiskDescription: Inspectors may not be able to effectively identify emerging food safety risks if they do
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a tracking system to monitor and remind inspectors of upcoming field i
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1148:
RiskId: 1400

ComplianceId: 2052
RiskTitle: Outdated Knowledge and Skills
Criticality: High
PossibleDamage: Increased risk of errors in inspection processes
Category: Operational
RiskType: Current
BusinessImpact: Potential health hazards for consumers
RiskDescription: Failure to complete required contact hours may result in inspectors lacking updated k
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide access to approved training programs and workshops for inspectors", "2"
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1149:
RiskId: 1401
ComplianceId: 2053
RiskTitle: Incomplete Coursework
Criticality: High
PossibleDamage: Inadequate training and knowledge for inspectors, potentially leading to errors in ins
Category: Operational
RiskType: Current
BusinessImpact: Quality and accuracy of food inspections may be compromised, affecting public healt
RiskDescription: Failure to complete required coursework within the specified timeframe may result in i
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Provide additional training opportunities for inspectors who may need more time t
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1150:
RiskId: 1402
ComplianceId: 2054
RiskTitle: Incomplete Training for Inspectors
Criticality: High
PossibleDamage: Inadequate knowledge and skills for inspectors
Category: Operational
RiskType: Inherent
BusinessImpact: Potential compromise of food inspection operations and public health
RiskDescription: Inspectors may lack the necessary training to effectively perform inspections, leading
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reminders and notifications to inspectors about upcoming course deadlin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1151:
RiskId: 1403
ComplianceId: 2055
RiskTitle: Outdated Training Resources
Criticality: Medium
PossibleDamage: Access to outdated or irrelevant training resources

Category: Operational
RiskType: Inherent
BusinessImpact: Compromised training effectiveness and inspector competency
RiskDescription: Inspectors may access outdated or irrelevant training resources, leading to gaps in kn
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update of online course list based on industry standards and
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1152:
RiskId: 1404
ComplianceId: 2056
RiskTitle: Outdated Knowledge and Incorrect Inspections
Criticality: High
PossibleDamage: Incorrect inspections may lead to health risks to the public
Category: Operational
RiskType: Inherent
BusinessImpact: Compromised food safety standards
RiskDescription: Failure to complete required continuing education may result in inspectors lacking upd
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide access to relevant training resources", "2": "Implement a tracking system
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1153:
RiskId: 1405
ComplianceId: 2057
RiskTitle: Incomplete Records and Non-Compliance
Criticality: Medium
PossibleDamage: Incomplete records may lead to non-compliance with ongoing education requiremen
Category: Operational
RiskType: Inherent
BusinessImpact: Potential non-compliance with industry standards
RiskDescription: Failure to submit proof of completed courses may result in incomplete records, leadin
RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a clear submission process for inspectors to follow", "2": "Provide remin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1154:
RiskId: 1406
ComplianceId: 2058
RiskTitle: Inaccurate Food Plant Classification
Criticality: High
PossibleDamage: Potential food safety hazards due to inadequate inspection of high-risk food plants
Category: Operational
RiskType: Inherent
BusinessImpact: Increased risk of foodborne illness outbreaks
RiskDescription: Failure to accurately classify food plants based on risk factors may lead to insufficient

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for inspectors on inventory maintenance procedures", "2": "Autom
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1155:
RiskId: 1407
ComplianceId: 2059
RiskTitle: Insufficient Inspection Frequency
Criticality: Medium
PossibleDamage: Undetected food safety issues due to infrequent inspections, leading to public health
Category: Operational
RiskType: Inherent
BusinessImpact: Increased risk of public health hazards
RiskDescription: Failure to conduct inspections as per the risk assessment may result in undetected fo
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular risk assessment updates for inspection frequency determination", "2": "Pr
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1156:
RiskId: 1408

ComplianceId: 2060
RiskTitle: Delayed Submission of Inspection Reports
Criticality: High
PossibleDamage: Regulatory penalties, missed follow-up actions, compromised data integrity
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of inspection processes, potential legal consequences
RiskDescription: Failure to submit inspection reports within the specified timeframe may result in regula
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reminders for report submission deadlines", "2": "Provide tr
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1157:
RiskId: 1409
ComplianceId: 2061
RiskTitle: Delayed Communication of Recalls
Criticality: High
PossibleDamage: Health risks, legal penalties, reputation damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential lawsuits, fines, loss of consumer trust
RiskDescription: Failure to communicate recalls promptly may result in widespread consumption of cor
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear communication protocols and contact lists", "2": "Conduct regular t

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 1158:

RiskId: 1410

ComplianceId: 2062

RiskTitle: Inadequate Documentation of Recall Process

Criticality: Medium

PossibleDamage: Regulatory fines, legal disputes, operational inefficiencies

Category: Operational

RiskType: Inherent

BusinessImpact: Loss of credibility, financial penalties

RiskDescription: Lack of proper documentation may result in difficulties in tracking recalled products, n

RiskLikelihood: 6

RiskImpact: 8

RiskExposureRating: 48

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement a standardized documentation template for recalls", "2": "Regularly rev

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1159:

RiskId: 1411

ComplianceId: 2063

RiskTitle: Delayed Consumer Complaint Acknowledgement

Criticality: High

PossibleDamage: Negative impact on consumer trust and reputation

Category: Operational
RiskType: Inherent
BusinessImpact: Increased complaints, regulatory fines
RiskDescription: Failure to acknowledge consumer complaints within 24 hours may lead to dissatisfact
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated acknowledgment system", "2": "Establish escalation proces
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1160:
RiskId: 1412
ComplianceId: 2064
RiskTitle: Delayed Consumer Complaint Resolution
Criticality: High
PossibleDamage: Legal action, financial penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Legal disputes, financial losses
RiskDescription: Failure to resolve consumer complaints within 10 business days may lead to escalatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear resolution process", "2": "Regular follow-ups with complainants", "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1161:
RiskId: 1413
ComplianceId: 2065
RiskTitle: Failure to Conduct Annual Risk Assessment
Criticality: High
PossibleDamage: Inadequate inspection prioritization and increased risk of food safety incidents
Category: Operational
RiskType: Inherent
BusinessImpact: Potential harm to consumers, regulatory fines, and damage to reputation
RiskDescription: Not conducting annual risk assessments may result in overlooking critical risk factors
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reminders for annual assessments", "2": "Provide training c
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1162:
RiskId: 1414
ComplianceId: 2066
RiskTitle: Ineffective Utilization of Risk Assessment Tool
Criticality: Medium
PossibleDamage: Inaccurate risk assessments and ineffective inspection prioritization
Category: Operational
RiskType: Inherent
BusinessImpact: Potential regulatory fines and compromised food safety
RiskDescription: Failure to utilize the standardized risk assessment tool may result in inconsistent risk

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update the risk assessment tool based on industry standards", "2": "Pro
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1163:
RiskId: 1415
ComplianceId: 2067
RiskTitle: Inadequate Inspection Frequency
Criticality: High
PossibleDamage: Increased risk of food safety hazards and potential regulatory non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Potential foodborne illness outbreaks, product recalls, and reputational damage
RiskDescription: Inadequate inspection frequency may result in undetected food safety hazards in high
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and adjustment of inspection schedules based on risk assessmen
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1164:
RiskId: 1416

ComplianceId: 2068
RiskTitle: Lack of Qualified Auditors for Field Inspection Audits
Criticality: High
PossibleDamage: Inaccurate audit findings and potential non-compliance issues
Category: Compliance
RiskType: Current
BusinessImpact: State agency inspection credibility and regulatory compliance
RiskDescription: Using unqualified auditors may lead to audit errors, missed compliance issues, and re
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and certification programs for auditors", "2": "Implement a peer re
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1165:
RiskId: 1417
ComplianceId: 2069
RiskTitle: Failure to Identify Key Material Topics
Criticality: High
PossibleDamage: Impact on organizational sustainability performance and stakeholder trust
Category: Operational
RiskType: Inherent
BusinessImpact: Reduced credibility, stakeholder dissatisfaction, potential regulatory non-compliance
RiskDescription: Failure to engage stakeholders effectively may result in overlooking critical material to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular stakeholder engagement sessions", "2": "Diverse engagement methods",
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1166:
RiskId: 1418
ComplianceId: 2070
RiskTitle: Inadequate Impact Assessment of Changes
Criticality: Medium
PossibleDamage: Misidentification of material topics impacting organizational sustainability
Category: Operational
RiskType: Inherent
BusinessImpact: Suboptimal decision-making, resource misallocation, missed opportunities
RiskDescription: Delay or inadequate assessment of impacts may lead to overlooking critical material t
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear criteria for triggering assessments", "2": "Dedicated resources for timely ass
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1167:
RiskId: 1419
ComplianceId: 2071
RiskTitle: Inaccurate GRI Reporting
Criticality: High
PossibleDamage: Legal penalties, loss of credibility, reputational damage

Category: Compliance
RiskType: Current
BusinessImpact: Potential legal actions and damage to reputation
RiskDescription: Failure to comply with GRI Standards in reporting leading to inaccurate disclosures ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GRI Standards for reporting team", "2": "Internal audits to veri
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1168:
RiskId: 1420
ComplianceId: 2072
RiskTitle: Omission Justification Failure
Criticality: Medium
PossibleDamage: Stakeholder distrust, legal challenges, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Loss of stakeholder trust and potential legal actions
RiskDescription: Failure to provide adequate justification for omissions in the sustainability report leadi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear documentation of reasons for omissions", "2": "Review by compliance office
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1169:
RiskId: 1421
ComplianceId: 2073
RiskTitle: Inaccurate Material Topic Identification
Criticality: High
PossibleDamage: Misalignment with organizational goals, regulatory non-compliance, reputational dam
Category: Operational
RiskType: Inherent
BusinessImpact: Impacts decision-making processes, sustainability reporting accuracy, and stakeholde
RiskDescription: Failure to accurately identify material topics can lead to misinformed decision-making
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review stakeholder engagement processes for effectiveness", "2": "Prov
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1170:
RiskId: 1422
ComplianceId: 2074
RiskTitle: Inadequate Stakeholder Engagement
Criticality: High
PossibleDamage: Reputational damage, loss of stakeholder trust, regulatory fines
Category: Reputational
RiskType: Residual
BusinessImpact: Impacts all business units involved in stakeholder engagement and sustainability repo
RiskDescription: Failure to engage stakeholders effectively may result in inaccurate or incomplete sust

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update stakeholder engagement methods", "2": "Provide tra
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1171:
RiskId: 1423
ComplianceId: 2075
RiskTitle: Unidentified Negative Impacts
Criticality: High
PossibleDamage: Reputational damage, legal consequences, environmental harm, economic losses
Category: Operational
RiskType: Inherent
BusinessImpact: All business units within the organization
RiskDescription: Failure to conduct the annual impact assessment may result in unidentified negative i
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure all relevant departments participate in the assessment process", "2": "Utili
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1172:
RiskId: 1424

ComplianceId: 2076
RiskTitle: Stakeholder Disengagement
Criticality: High
PossibleDamage: Loss of reputation, legal disputes, operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of stakeholder trust and support, leading to financial and operational ch
RiskDescription: Failure to engage with stakeholders effectively may result in misunderstandings, confl
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular stakeholder engagement activities", "2": "Transparent communication of
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1173:
RiskId: 1425
ComplianceId: 2077
RiskTitle: Lack of Stakeholder Engagement
Criticality: High
PossibleDamage: Reputational damage, loss of community support, legal challenges
Category: Reputational
RiskType: Current
BusinessImpact: Potential loss of business opportunities, decreased customer loyalty, negative impact
RiskDescription: Failure to engage stakeholders may result in decisions that do not consider their inter
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear communication channels for stakeholders to provide feedback", "2

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 1174:

RiskId: 1426

ComplianceId: 2078

RiskTitle: Lack of Documentation in Stakeholder Engagements

Criticality: Medium

PossibleDamage: Misunderstandings, disputes with stakeholders, lack of transparency

Category: Operational

RiskType: Current

BusinessImpact: Potential breakdown in stakeholder trust, difficulty in addressing stakeholder concern

RiskDescription: Failure to document stakeholder engagements may lead to disputes over the organiza

RiskLikelihood: 5

RiskImpact: 7

RiskExposureRating: 35

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement a centralized system for recording stakeholder engagements and feed

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 1175:

RiskId: 1427

ComplianceId: 2079

RiskTitle: Negative Human Rights Impacts on Stakeholders

Criticality: High

PossibleDamage: Reputational damage, legal liabilities, loss of stakeholder trust

Category: Compliance
RiskType: Inherent
BusinessImpact: Potential lawsuits, fines, and harm to stakeholders
RiskDescription: Failure to conduct human rights impact assessments may result in negative impacts c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear assessment guidelines and timelines", "2": "Engage with stakehold
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1176:
RiskId: 1428
ComplianceId: 2080
RiskTitle: Outdated Human Rights Impact Assessments
Criticality: Medium
PossibleDamage: Ineffective mitigation strategies, unaddressed human rights impacts
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential human rights violations and reputational damage
RiskDescription: Failure to review human rights impact assessments annually may result in outdated m
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a regular review schedule for assessments", "2": "Engage with stakehol
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1177:
RiskId: 1429
ComplianceId: 2081
RiskTitle: Misinterpretation of Reporting Principles
Criticality: High
PossibleDamage: Inaccurate reporting and potential legal consequences
Category: Compliance
RiskType: Residual
BusinessImpact: All business units involved in reporting activities
RiskDescription: Failure to apply GRI reporting principles correctly leading to inaccurate reporting, pote
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular refresher training sessions", "2": "Mentoring by experienced team membe
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1178:
RiskId: 1430
ComplianceId: 2082
RiskTitle: Inconsistent Reporting Practices
Criticality: Critical
PossibleDamage: Loss of stakeholder trust and credibility
Category: Compliance
RiskType: Residual
BusinessImpact: All business units involved in reporting activities
RiskDescription: Failure to consistently apply GRI reporting principles leading to incomplete or inaccura

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting guidelines", "2": "Regular reviews of reported data", "3":
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1179:
RiskId: 1431
ComplianceId: 2083
RiskTitle: Inaccurate Sustainability Reporting
Criticality: High
PossibleDamage: Loss of stakeholder trust, reputational damage, regulatory scrutiny
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, decreased investor confidence, negative media coverage
RiskDescription: Failure to accurately report material topics can lead to misinformed decision-making b
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear criteria for material topic determination", "2": "Regularly review and
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1180:
RiskId: 1432

ComplianceId: 2084
RiskTitle: Non-Compliance with Annual Reporting of Disclosures
Criticality: High
PossibleDamage: Risk of regulatory fines, reputational damage, and loss of stakeholder trust
Category: Compliance
RiskType: Current
BusinessImpact: Potential financial penalties and damage to organizational reputation
RiskDescription: Failure to report disclosures annually as per GRI 2 and GRI 3 may lead to regulatory
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust internal audit process to ensure all disclosures are captured a
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1181:
RiskId: 1433
ComplianceId: 2085
RiskTitle: Incomplete or Inaccurate Disclosures
Criticality: High
PossibleDamage: Legal actions, fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: All business units involved in sustainability reporting
RiskDescription: Failure to conduct the annual assessment of material topics may lead to incomplete o
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement a reminder system to ensure timely completion of the assessment", "2
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1182:
RiskId: 1434
ComplianceId: 2086
RiskTitle: Challenges in Justifying Selected Disclosures
Criticality: Medium
PossibleDamage: Stakeholder questions, reputational risks
Category: Compliance
RiskType: Current
BusinessImpact: All business units involved in sustainability reporting
RiskDescription: Failure to document the rationale for selected disclosures may result in challenges in
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear documentation guidelines for rationale recording", "2": "Conduct re
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1183:
RiskId: 1435
ComplianceId: 2087
RiskTitle: Inaccurate Reporting Due to Omission
Criticality: High
PossibleDamage: Loss of stakeholder trust, legal fines, reputational damage

Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal consequences, loss of credibility, stakeholder backlash
RiskDescription: Failure to document reasons for omission may result in inaccurate reporting, leading t
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GRI Standards and reporting requirements", "2": "Internal aud
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1184:
RiskId: 1436
ComplianceId: 2088
RiskTitle: Inaccurate Omission Reason Documentation
Criticality: High
PossibleDamage: Loss of stakeholder trust and reputation damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Negative impact on organizational reputation and credibility
RiskDescription: Failure to accurately document omission reasons may lead to misinterpretation of sus
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear documentation guidelines for omission reasons", "2": "Implement r
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1185:
RiskId: 1437
ComplianceId: 2089
RiskTitle: Incomplete GRI Content Index
Criticality: High
PossibleDamage: Loss of stakeholder trust and credibility, regulatory fines
Category: Compliance
RiskType: Inherent
BusinessImpact: Negative impact on reputation and relationships with stakeholders
RiskDescription: Failure to accurately summarize reported information, disclose necessary details, or c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GRI Standards and reporting requirements", "2": "Internal aud
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1186:
RiskId: 1438
ComplianceId: 2090
RiskTitle: Exclusion from GRI Recognition
Criticality: High
PossibleDamage: Reputational damage and missed opportunities for collaboration with GRI
Category: Reputational
RiskType: Inherent
BusinessImpact: Reputational damage affecting the organization's credibility in sustainability reporting
RiskDescription: Failure to notify GRI of the organization's use of the GRI Standards may result in excl

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely submission of the notification email within the specified timeframe",
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1187:
RiskId: 1439
ComplianceId: 2091
RiskTitle: Misalignment with GRI Standards
Criticality: High
PossibleDamage: Reputational damage, loss of stakeholder trust, legal implications
Category: Compliance
RiskType: Current
BusinessImpact: Negative impact on stakeholder relations, potential legal consequences
RiskDescription: Failure to align with GRI Standards in reporting may lead to misinterpretation of data a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GRI Standards for reporting staff", "2": "Internal audits to ensu
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1188:
RiskId: 1440

ComplianceId: 2092
RiskTitle: Inaccurate Financial Reporting
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Incorrect financial decisions, loss of investor trust
RiskDescription: Incorrect financial data leading to incorrect analysis and decision-making
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reconciliation of financial data", "2": "Internal and external audits", "3": "C
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1189:
RiskId: 1441
ComplianceId: 2093
RiskTitle: Misleading Stakeholders
Criticality: Medium
PossibleDamage: Loss of stakeholder trust, regulatory fines
Category: Compliance
RiskType: Current
BusinessImpact: Negative perception, reduced investor confidence
RiskDescription: Publication of inaccurate sustainability information leading to incorrect stakeholder pe
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Stakeholder engagement on reporting accuracy", "2": "Regular review of sustaina
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1190:
RiskId: 1442
ComplianceId: 2094
RiskTitle: Misleading Stakeholders Due to Unbalanced Reporting
Criticality: High
PossibleDamage: Reputational damage, loss of stakeholder trust
Category: Reputational
RiskType: Current
BusinessImpact: Negative impact on stakeholder relationships and organizational reputation
RiskDescription: Failure to include both positive and negative impacts in sustainability reporting may le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust review processes for sustainability reporting", "2": "Provide trair
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1191:
RiskId: 1443
ComplianceId: 2095
RiskTitle: Difficulty in Navigating Sustainability Reports
Criticality: High
PossibleDamage: Decreased understanding of sustainability information, misinterpretation of data

Category: Operational
RiskType: Current
BusinessImpact: May impact decision-making processes based on inaccurate interpretation of sustaina
RiskDescription: Users may struggle to locate specific information within the report due to the absence
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a clear and detailed table of contents in all sustainability reports", "2": "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1192:
RiskId: 1444
ComplianceId: 2096
RiskTitle: Difficulty in Interpreting Complex Sustainability Data
Criticality: Medium
PossibleDamage: Reduced clarity and understanding of sustainability information
Category: Operational
RiskType: Current
BusinessImpact: May impact decision-making processes based on inaccurate interpretation of comple
RiskDescription: Users may find it challenging to interpret complex sustainability data without visual aid
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Incorporate a variety of visual aids in sustainability reports to enhance compreher
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 1193:
RiskId: 1445
ComplianceId: 2097
RiskTitle: Inconsistent Reporting Metrics
Criticality: High
PossibleDamage: Inaccurate comparisons and misinterpretation of sustainability performance
Category: Compliance
RiskType: Current
BusinessImpact: All business units involved in sustainability reporting
RiskDescription: Failure to adopt standard metrics and methodologies may lead to inconsistent reporti
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on standardized metrics", "2": "Centralized repository fo
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1194:
RiskId: 1446
ComplianceId: 2098
RiskTitle: Inaccurate Data Reporting
Criticality: High
PossibleDamage: Misrepresentation of data leading to inaccurate reporting
Category: Operational
RiskType: Residual
BusinessImpact: Loss of stakeholder trust and credibility
RiskDescription: Failure to accurately consolidate data may result in misleading sustainability reports, c

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of data consolidation process", "2": "Training on proper data conso
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1195:
RiskId: 1447
ComplianceId: 2099
RiskTitle: Inconsistent Omission Reporting
Criticality: Medium
PossibleDamage: Lack of transparency in reporting leading to credibility issues
Category: Operational
RiskType: Residual
BusinessImpact: Questions about data integrity and credibility of sustainability reports
RiskDescription: Failure to standardize omission reporting may result in inconsistencies, raising doubts
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear guidelines for reporting omissions", "2": "Regular review of omissio
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1196:
RiskId: 1448

ComplianceId: 2100
RiskTitle: Misrepresentation of Organizational Details
Criticality: High
PossibleDamage: Legal consequences, loss of credibility, financial penalties
Category: Compliance
RiskType: Residual
BusinessImpact: Impact on regulatory compliance and stakeholder trust
RiskDescription: Failure to accurately disclose legal name and ownership details can lead to legal and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for accurate reporting", "2": "Internal audit checks for verification"
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1197:
RiskId: 1449
ComplianceId: 2101
RiskTitle: Inaccurate Entities in Sustainability Reporting
Criticality: High
PossibleDamage: Loss of credibility, legal fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal actions, financial penalties, damage to reputation
RiskDescription: Incorrect entities included in sustainability reporting leading to misrepresentation of or
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular audits to verify accuracy of entity list", "2": "Training for staff involved in c
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1198:
RiskId: 1450
ComplianceId: 2102
RiskTitle: Misleading Reporting Period Disclosure
Criticality: High
PossibleDamage: Loss of stakeholder trust and credibility in sustainability reporting
Category: Operational
RiskType: Current
BusinessImpact: Potential negative impact on organizational reputation and stakeholder relationships
RiskDescription: Incorrectly disclosing the reporting period may lead to misinterpretation of sustainabili
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust review processes for reporting period disclosure", "2": "Provide
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1199:
RiskId: 1451
ComplianceId: 2103
RiskTitle: Inadequate Contact Point Disclosure
Criticality: Medium
PossibleDamage: Missed opportunities for stakeholder engagement and communication

Category: Operational
RiskType: Current
BusinessImpact: Potential negative impact on stakeholder relationships and communication
RiskDescription: Failing to provide a designated contact point may result in missed opportunities to eng
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels for inquiries", "2": "Train designated cont
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1200:
RiskId: 1452
ComplianceId: 2104
RiskTitle: Misleading Sustainability Reporting
Criticality: High
PossibleDamage: Loss of stakeholder trust, legal consequences, financial penalties
Category: Compliance
RiskType: Current
BusinessImpact: Negative impact on organizational reputation, stakeholder relationships, and financial
RiskDescription: Failure to accurately disclose entities in sustainability reporting can lead to misleading
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to verify accuracy of disclosed entities", "2": "Training for sustainab
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1201:
RiskId: 1453
ComplianceId: 2105
RiskTitle: Outdated Entity List in Sustainability Reporting
Criticality: Medium
PossibleDamage: Misinformed stakeholders, inaccurate reporting, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential misinterpretation of organizational activities and structure by stakeholders
RiskDescription: Failure to update the entity list in sustainability reporting following organizational chan
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a process for immediate updates to the entity list post-organizational ch
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1202:
RiskId: 1454
ComplianceId: 2106
RiskTitle: Misalignment of Reporting Periods
Criticality: High
PossibleDamage: Confusion and inconsistency in reporting, potential investor distrust
Category: Operational
RiskType: Current
BusinessImpact: Delayed decision-making, inaccurate financial analysis
RiskDescription: Failure to align reporting periods may result in discrepancies between financial and su

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly communicate any changes in reporting period", "2": "Provide detailed ra
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1203:
RiskId: 1455
ComplianceId: 2107
RiskTitle: Unclear Reporting Frequency
Criticality: Medium
PossibleDamage: Missed deadlines, incomplete reports, stakeholder confusion
Category: Operational
RiskType: Current
BusinessImpact: Delayed reporting, inaccurate data analysis
RiskDescription: Failure to specify reporting frequency may result in missed deadlines, incomplete repo
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting schedule with deadlines", "2": "Regularly communicate r
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1204:
RiskId: 1456

ComplianceId: 2108
RiskTitle: Misleading Stakeholders
Criticality: High
PossibleDamage: Loss of credibility, legal consequences
Category: Compliance
RiskType: Current
BusinessImpact: Potential loss of trust from stakeholders, legal actions
RiskDescription: Failure to accurately document restatements can lead to misleading stakeholders and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust internal controls for data accuracy", "2": "Regularly review and v
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1205:
RiskId: 1457
ComplianceId: 2109
RiskTitle: Confusion Among Stakeholders
Criticality: Medium
PossibleDamage: Loss of stakeholder trust, misinterpretation of information
Category: Compliance
RiskType: Current
BusinessImpact: Potential misinterpretation of restatement reasons and effects
RiskDescription: Inadequate explanation of restatements can lead to confusion among stakeholders ar
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Provide training to reporting team on clear communication", "2": "Engage with sta
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1206:
RiskId: 1458
ComplianceId: 2110
RiskTitle: Lack of External Assurance Transparency
Criticality: High
PossibleDamage: Loss of credibility and trust from stakeholders
Category: Compliance
RiskType: Current
BusinessImpact: Loss of stakeholder trust and potential negative impact on organizational reputation
RiskDescription: Failure to provide clear external assurance policy and reports may lead to doubts abo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of external assurance process", "2": "Training for governance bodi
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1207:
RiskId: 1459
ComplianceId: 2111
RiskTitle: Lack of Governance Oversight in External Assurance
Criticality: Medium
PossibleDamage: Inaccurate external assurance and potential legal or reputational risks

Category: Compliance
RiskType: Current
BusinessImpact: Potential legal and reputational risks for governance body and senior executives
RiskDescription: Failure to provide oversight in the external assurance process may result in inaccurat
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear roles and responsibilities for governance body and senior executiv
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1208:
RiskId: 1460
ComplianceId: 2112
RiskTitle: Compromised Assurance Provider Independence
Criticality: High
PossibleDamage: Loss of credibility in sustainability reporting
Category: Compliance
RiskType: Inherent
BusinessImpact: Impacts decision-making based on sustainability reports
RiskDescription: Failure to ensure independence of assurance provider can lead to biased reporting ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear independence criteria", "2": "Regularly monitor assurance provide
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1209:
RiskId: 1461
ComplianceId: 2113
RiskTitle: Inaccurate Value Chain Reporting
Criticality: High
PossibleDamage: Loss of stakeholder trust and regulatory fines
Category: Compliance
RiskType: Residual
BusinessImpact: Loss of credibility and financial penalties
RiskDescription: Failure to accurately report value chain activities could lead to misinformed stakehold
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular internal audits to ensure accuracy of reported information", "2"
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1210:
RiskId: 1462
ComplianceId: 2114
RiskTitle: Failure to Report Significant Changes
Criticality: Medium
PossibleDamage: Loss of stakeholder trust and regulatory fines
Category: Compliance
RiskType: Residual
BusinessImpact: Loss of credibility and financial penalties
RiskDescription: Not reporting significant changes in the value chain could lead to misinformed stakeho

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear criteria for defining 'significant changes' in the value chain", "2": "In
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1211:
RiskId: 1463
ComplianceId: 2115
RiskTitle: Inaccurate Reporting of Employee Counts
Criticality: High
PossibleDamage: Misrepresentation of employee demographics leading to loss of stakeholder trust an
Category: Compliance
RiskType: Current
BusinessImpact: All business units would be impacted by potential legal and reputational consequence
RiskDescription: Failure to accurately report employee counts and breakdowns could result in misinfor
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular data quality checks to ensure accuracy of reported data", "2": "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1212:
RiskId: 1464

ComplianceId: 2116
RiskTitle: Misinterpretation of Employee Data
Criticality: Medium
PossibleDamage: Misinterpretation of reported data leading to incorrect assumptions and decisions
Category: Compliance
RiskType: Current
BusinessImpact: All business units would be impacted by misinterpretation of reported data
RiskDescription: Failure to provide contextual information in employee reports could result in stakehold
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Include clear explanations for any significant fluctuations in employee data", "2": "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1213:
RiskId: 1465
ComplianceId: 2117
RiskTitle: Inaccurate Employee Data Reporting
Criticality: High
PossibleDamage: Incorrect reporting may lead to financial penalties and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial penalties, reputational damage
RiskDescription: Inaccurate employee data reporting may result in non-compliance with GRI standards
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular data audits", "2": "Training on data collection procedures", "3": "Implemer

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 1214:

RiskId: 1466

ComplianceId: 2118

RiskTitle: Late Employee Data Reporting

Criticality: Medium

PossibleDamage: Late reporting may lead to penalties and impact decision-making processes

Category: Compliance

RiskType: Current

BusinessImpact: Penalties, delayed decision-making

RiskDescription: Late reporting of employee data may result in non-compliance with reporting requirem

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear reporting deadlines", "2": "Implement reminders and notifications f

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1215:

RiskId: 1467

ComplianceId: 2119

RiskTitle: Misinterpretation of Employee Data

Criticality: High

PossibleDamage: Incorrect decision-making based on misinterpreted data

Category: Operational
RiskType: Current
BusinessImpact: Could lead to skewed workforce planning and ineffective resource allocation
RiskDescription: Failure to provide accurate contextual information alongside quantitative employee da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training to HR and reporting team on how to effectively include contextua
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1216:
RiskId: 1468
ComplianceId: 2120
RiskTitle: Inaccurate Non-Employee Worker Data Reporting
Criticality: High
PossibleDamage: Mismanagement of non-employee worker relationships, legal issues, and financial ri
Category: Operational
RiskType: Residual
BusinessImpact: Potential legal disputes, financial penalties, and operational disruptions
RiskDescription: Failure to accurately report non-employee worker data may result in mismanagement
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR and project managers on data collection procedures", "2":
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1217:
RiskId: 1469
ComplianceId: 2121
RiskTitle: Inconsistent Non-Employee Worker Data Reporting Templates
Criticality: Medium
PossibleDamage: Inconsistencies, errors, and difficulties in data analysis and decision-making
Category: Operational
RiskType: Residual
BusinessImpact: Inaccurate analysis and decision-making due to non-standardized data reporting
RiskDescription: Varied template usage for non-employee worker data reporting may lead to inconsiste
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide training on template usage to relevant staff", "2": "Regularly update templ
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1218:
RiskId: 1470
ComplianceId: 2122
RiskTitle: Misinterpretation of Non-Employee Worker Data
Criticality: High
PossibleDamage: Inaccurate reporting and decision-making
Category: Operational
RiskType: Current
BusinessImpact: Potential fines, reputational damage, and loss of stakeholder trust
RiskDescription: Failure to include accurate contextual information alongside quantitative data on non-

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training to HR and sustainability reporting team on how to effectively inclu
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1219:
RiskId: 1471
ComplianceId: 2123
RiskTitle: Inaccurate Reporting of Non-Employee Worker Numbers
Criticality: High
PossibleDamage: Non-compliance penalties, misallocation of resources, incorrect strategic decisions
Category: Operational
RiskType: Current
BusinessImpact: HR, Finance, and Operations departments would face challenges in resource allocati
RiskDescription: Failure to accurately report non-employee worker numbers could result in penalties, n
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of headcount data to ensure accuracy", "2": "Training HR staff on p
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1220:
RiskId: 1472

ComplianceId: 2124
RiskTitle: Incorrect FTE Calculations for Non-Employee Workers
Criticality: Medium
PossibleDamage: Inaccurate workforce planning, budgeting, compliance reporting
Category: Operational
RiskType: Current
BusinessImpact: HR department would face challenges in workforce planning, budgeting, and complia
RiskDescription: Incorrect FTE calculations may result in inaccurate workforce planning, budgeting, an
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Training HR staff on FTE calculation methods", "2": "Regular validation of FTE ca
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1221:
RiskId: 1473
ComplianceId: 2125
RiskTitle: Misclassification of Non-Employee Workers
Criticality: High
PossibleDamage: Legal disputes, financial penalties, and reputational damage
Category: Legal
RiskType: Inherent
BusinessImpact: Potential legal costs, fines, and damage to the organization's reputation
RiskDescription: Misclassification of non-employee workers can result in legal disputes over employme
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training for managers on control criteria", "2": "Legal review of control ass
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1222:
RiskId: 1474
ComplianceId: 2126
RiskTitle: Inaccurate Reporting of Non-Employee Worker Numbers
Criticality: High
PossibleDamage: Financial penalties, misallocation of resources, and decreased operational efficiency
Category: Operational
RiskType: Current
BusinessImpact: Misalignment with business needs, potential legal issues, and decreased operational
RiskDescription: Failure to accurately report fluctuations in non-employee worker numbers can lead to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for HR staff on data analysis and reporting procedures", "2": "Imp
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1223:
RiskId: 1475
ComplianceId: 2127
RiskTitle: Lack of Transparency in Sustainability Oversight
Criticality: High
PossibleDamage: Legal investigations, stakeholder distrust, negative media coverage

Category: Compliance
RiskType: Residual
BusinessImpact: Governance and compliance departments
RiskDescription: Failure to disclose governance committees responsible for sustainability oversight ma
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of committee information", "2": "Internal audits to verif
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1224:
RiskId: 1476
ComplianceId: 2128
RiskTitle: Misrepresentation of Governance Body Composition
Criticality: High
PossibleDamage: Reputational damage, legal fines, and loss of stakeholder trust
Category: Compliance
RiskType: Current
BusinessImpact: Potential legal and financial repercussions for the organization
RiskDescription: Misrepresentation of governance body composition can lead to allegations of discrimi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training on diversity and inclusion for governance members", "2
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1225:
RiskId: 1477
ComplianceId: 2129
RiskTitle: Stakeholder Exclusion Risk
Criticality: High
PossibleDamage: Decreased stakeholder trust and alignment with stakeholder expectations
Category: Operational
RiskType: Inherent
BusinessImpact: Governance and stakeholder relations departments
RiskDescription: Failure to engage stakeholders in the nomination process may lead to perceptions of
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly communicate with stakeholders to understand their expectations", "2": "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1226:
RiskId: 1478
ComplianceId: 2130
RiskTitle: Regional Stakeholder Exclusion Risk
Criticality: Medium
PossibleDamage: Limited diversity of perspectives in the nomination process
Category: Operational
RiskType: Inherent
BusinessImpact: All operational regions
RiskDescription: Failure to engage stakeholders from all regions may result in biases towards certain p

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Promote digital platform usage among stakeholders", "2": "Provide training on dig
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1227:
RiskId: 1479
ComplianceId: 2131
RiskTitle: Lack of Diversity in Governance Body
Criticality: High
PossibleDamage: Reduced effectiveness in decision-making and increased conflicts of interest
Category: Operational
RiskType: Inherent
BusinessImpact: May lead to biased decision-making, lack of innovation, and reputational damage
RiskDescription: Failure to have diverse perspectives in the governance body may result in decisions t
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on diversity and inclusion for governance body members", "2": "E
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1228:
RiskId: 1480

ComplianceId: 2132
RiskTitle: Failure to Engage Stakeholders
Criticality: High
PossibleDamage: Loss of stakeholder trust, project delays, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may experience delays or cancellations in projects
RiskDescription: Failure to engage stakeholders may result in misalignment with stakeholder expectati
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a clear stakeholder engagement plan with defined timelines and respon
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1229:
RiskId: 1481
ComplianceId: 2133
RiskTitle: Delay in Integrating Engagement Results
Criticality: Medium
PossibleDamage: Outdated material topics assessment, ineffective decision-making
Category: Operational
RiskType: Inherent
BusinessImpact: Sustainability team and decision-making processes may be impacted by outdated ma
RiskDescription: Delay in integrating engagement results may lead to outdated or inaccurate material t
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish clear timelines for reviewing and integrating engagement results", "2": "I
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1230:
RiskId: 1482
ComplianceId: 2134
RiskTitle: Inaccurate Impact Assessment
Criticality: High
PossibleDamage: Overlooking significant impacts and potential reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may be affected by inaccurate impact assessments
RiskDescription: Failure to accurately assess impacts may result in the organization missing critical iss
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on impact assessment methodology", "2": "Internal audits to ensu
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1231:
RiskId: 1483
ComplianceId: 2135
RiskTitle: Outdated Impact Assessments
Criticality: Medium
PossibleDamage: Ineffective prioritization of impacts due to outdated information

Category: Operational
RiskType: Inherent
BusinessImpact: Sustainability department may struggle to address material impacts effectively
RiskDescription: Failure to conduct bi-annual assessments may lead to outdated information, hinderin
RiskLikelihood: 7
RiskImpact: 5
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing a clear schedule for assessments", "2": "Utilizing a mix of quantitative
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1232:
RiskId: 1484
ComplianceId: 2136
RiskTitle: Inaccurate Reporting due to Lack of Documentation
Criticality: High
PossibleDamage: Misleading stakeholders, legal implications, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of stakeholder trust, potential legal fines, reputational damage
RiskDescription: Failure to document the material topics determination process may result in inaccurat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation best practices", "2": "Internal audits to ensure
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1233:
RiskId: 1485
ComplianceId: 2137
RiskTitle: Misinformed Decision-Making due to Outdated Material Topics
Criticality: Medium
PossibleDamage: Inaccurate decision-making, stakeholder dissatisfaction, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate decisions, loss of stakeholder trust, reputational damage
RiskDescription: Failure to review material topics annually may result in outdated or irrelevant topics, le
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on material topics relevance criteria", "2": "External benchmarkin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1234:
RiskId: 1486
ComplianceId: 2138
RiskTitle: Misalignment with Key Stakeholders
Criticality: High
PossibleDamage: Loss of stakeholder trust, negative impact on reputation, misinformed decision-maki
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may experience disruptions in operations and decision-making proc
RiskDescription: Failure to identify key stakeholders and align organizational goals with stakeholder ex

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular communication with key stakeholders to gather feedback and updates", "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1235:
RiskId: 1487
ComplianceId: 2139
RiskTitle: Lack of Stakeholder Engagement
Criticality: High
PossibleDamage: Decreased trust, support, and alignment with stakeholder expectations
Category: Operational
RiskType: Residual
BusinessImpact: All business units and locations
RiskDescription: Failure to engage with stakeholders effectively may result in negative consequences s
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update stakeholder engagement strategy based on feedbac
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1236:
RiskId: 1488

ComplianceId: 2140
RiskTitle: Lack of Stakeholder Feedback
Criticality: High
PossibleDamage: Negative publicity and reputational damage
Category: Reputational
RiskType: Residual
BusinessImpact: Potential loss of stakeholder trust and support
RiskDescription: Failure to collect and consider stakeholder feedback may result in decisions that do n
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly communicate the availability of the feedback mechanism to stakeholder
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1237:
RiskId: 1489
ComplianceId: 2141
RiskTitle: Failure to Conduct Annual Impact Identification Process
Criticality: High
PossibleDamage: Unidentified risks and missed opportunities for improvement
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may be impacted by unidentified risks
RiskDescription: Failure to conduct the annual impact identification process may result in the organizat
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication and training on the impact identification process", "2
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1238:
RiskId: 1490
ComplianceId: 2142
RiskTitle: Ineffective Impact Evaluation Framework
Criticality: High
PossibleDamage: Misprioritization of risks, inadequate reporting, increased exposure to unidentified im
Category: Operational
RiskType: Inherent
BusinessImpact: Potential disruption to operations, financial losses, reputational damage.
RiskDescription: Failure to develop a structured impact evaluation framework may lead to ineffective ev
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on impact evaluation framework", "2": "Establish clear reporting r
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1239:
RiskId: 1491
ComplianceId: 2143
RiskTitle: Unidentified Negative Impacts
Criticality: High
PossibleDamage: Reputational damage, legal issues, financial losses

Category: Operational
RiskType: Inherent
BusinessImpact: Potential disruptions in operations and stakeholder trust
RiskDescription: Failure to identify negative impacts may lead to unforeseen consequences affecting th
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular impact assessment training programs", "2": "Automated impact assessm
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1240:
RiskId: 1492
ComplianceId: 2144
RiskTitle: Missed Positive Impact Identification
Criticality: High
PossibleDamage: Missed opportunities for sustainable development contributions and potential reputa
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to identify positive impacts may result in missed opportunities for sustainable d
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for impact identification techniques", "2": "Implement automated t
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1241:
RiskId: 1493
ComplianceId: 2145
RiskTitle: Misalignment of Actions with Impact Significance
Criticality: High
PossibleDamage: Inaccurate prioritization of actions and reporting, potential reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption in operational efficiency and potential stakeholder dissatisfaction
RiskDescription: Failure to align actions with impact significance assessment results may lead to ineffi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on impact assessment criteria", "2": "Internal audits to ensure co
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1242:
RiskId: 1494
ComplianceId: 2146
RiskTitle: Incomplete Stakeholder Identification
Criticality: High
PossibleDamage: Misinformed impact assessments and lack of stakeholder engagement.
Category: Operational
RiskType: Inherent
BusinessImpact: All business units involved in sustainability reporting.
RiskDescription: Failure to identify key stakeholders may result in incomplete impact assessments, lea

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular stakeholder mapping exercises", "2": "Utilization of stakeholder engagem
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1243:
RiskId: 1495
ComplianceId: 2147
RiskTitle: Infrequent Stakeholder Engagement
Criticality: Medium
PossibleDamage: Outdated impact assessments and lack of stakeholder input.
Category: Operational
RiskType: Inherent
BusinessImpact: All business units involved in sustainability reporting.
RiskDescription: Infrequent stakeholder engagement may result in outdated impact assessments, lead
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing a stakeholder engagement calendar", "2": "Utilizing diverse engagem
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1244:
RiskId: 1496

ComplianceId: 2148
RiskTitle: Inaccurate Impact Assessment
Criticality: High
PossibleDamage: Misaligned decision-making, regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, regulatory penalties, and damage to organizational reputati
RiskDescription: Failure to consult with experts may lead to inaccurate evaluation of impacts, resulting
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear criteria for expert selection and engagement", "2": "Regularly revie
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1245:
RiskId: 1497
ComplianceId: 2149
RiskTitle: Inaccurate Reporting Due to Undefined Threshold
Criticality: High
PossibleDamage: Misrepresentation of impacts, regulatory fines, loss of credibility
Category: Compliance
RiskType: Residual
BusinessImpact: May lead to legal consequences and reputational damage
RiskDescription: Failure to establish a clear threshold for material topics may result in inaccurate repor
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on threshold setting", "2": "Internal audits to verify compliance", "

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1246:

RiskId: 1498

ComplianceId: 2150

RiskTitle: Failure to Conduct Annual Stakeholder Engagement Survey

Criticality: High

PossibleDamage: Potential reputation damage and loss of stakeholder trust

Category: Operational

RiskType: Current

BusinessImpact: Loss of stakeholder trust, negative publicity, and legal/regulatory issues

RiskDescription: Not conducting the annual stakeholder engagement survey may result in overlooking

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Ensure clear communication and reminders about the survey timeline and importa

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1247:

RiskId: 1499

ComplianceId: 2151

RiskTitle: Lack of Stakeholder Engagement Documentation

Criticality: Medium

PossibleDamage: Unclear accountability and challenges in addressing stakeholder feedback effectivel

Category: Operational
RiskType: Current
BusinessImpact: Disputes with stakeholders, missed improvement opportunities, and challenges in de
RiskDescription: Failure to document the stakeholder engagement process may result in unclear accou
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear documentation procedures and templates for stakeholder engage
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1248:
RiskId: 1500
ComplianceId: 2152
RiskTitle: Loss of Credibility in Sustainability Reporting
Criticality: High
PossibleDamage: Loss of stakeholder trust, reputational damage, and decreased credibility in sustaina
Category: Compliance
RiskType: Inherent
BusinessImpact: Negative impact on stakeholder relationships, investor confidence, and brand reputat
RiskDescription: Failure to validate material topics externally may lead to inaccuracies, misinterpretatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly engage with diverse external experts and stakeholders for validation", "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1249:
RiskId: 1501
ComplianceId: 2153
RiskTitle: Non-Compliance with Reporting Standards
Criticality: High
PossibleDamage: Loss of credibility, regulatory fines, and reputational harm
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential financial penalties and damage to reputation
RiskDescription: Failure to comply with reporting standards could result in inaccurate disclosures, lead
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting guidelines and processes", "2": "Regular training and up
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1250:
RiskId: 1502
ComplianceId: 2154
RiskTitle: Stakeholder Engagement Risk
Criticality: High
PossibleDamage: Loss of stakeholder trust and support, reputational damage, disruption of operations
Category: Operational
RiskType: Residual
BusinessImpact: Potential impact on organizational reputation and relationships with key stakeholders
RiskDescription: Failure to effectively engage stakeholders could lead to conflicts, misalignment of prio

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular communication with stakeholders to address concerns", "2": "Establish cl
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1251:
RiskId: 1503
ComplianceId: 2155
RiskTitle: Failure to Conduct Impact Assessments
Criticality: High
PossibleDamage: Risk of overlooking critical issues that could harm the organization's reputation and s
Category: Operational
RiskType: Residual
BusinessImpact: Potential harm to the organization's reputation and sustainability efforts
RiskDescription: Failure to conduct impact assessments may lead to the organization missing critical is
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication and accountability for conducting assessments", "2":
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1252:
RiskId: 1504

ComplianceId: 2156
RiskTitle: Failure to Publish Annual Material Topics Report
Criticality: High
PossibleDamage: Reputational damage, loss of stakeholder trust, regulatory penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential negative impact on stakeholder relationships, brand reputation, and regulat
RiskDescription: Failure to publish the annual material topics report may lead to a lack of transparency
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting processes and timelines", "2": "Implement regular monit
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1253:
RiskId: 1505
ComplianceId: 2157
RiskTitle: Failure to Disclose Negative Impacts
Criticality: High
PossibleDamage: Reputational damage, loss of stakeholder trust, legal consequences
Category: Reputational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to disclose negative impacts can result in reputational damage, loss of stakeh
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear assessment criteria", "2": "Regularly review and update disclosure
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1254:
RiskId: 1506
ComplianceId: 2158
RiskTitle: Misrepresentation of Positive Impacts
Criticality: High
PossibleDamage: Loss of stakeholder trust, reputational damage, legal consequences
Category: Reputational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to accurately report positive impacts can lead to a loss of credibility and trust a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data verification processes", "2": "Regularly audit reporting accu
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1255:
RiskId: 1507
ComplianceId: 2159
RiskTitle: Ineffective Management Commitments
Criticality: High
PossibleDamage: Mismanagement of material topics and potential reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: All business units may be impacted by ineffective management commitments
RiskDescription: Failure to develop clear and documented management commitments may lead to mis
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and communication on the importance of management commitm
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1256:
RiskId: 1508
ComplianceId: 2160
RiskTitle: Lack of Executive Approval for Management Commitments
Criticality: Medium
PossibleDamage: Lack of commitment enforcement and accountability
Category: Operational
RiskType: Residual
BusinessImpact: All business units may be impacted by lack of executive approval
RiskDescription: Failure to obtain executive approval for management commitments may result in lack
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular communication on the importance of executive approval for commitments
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1257:
RiskId: 1509
ComplianceId: 2161
RiskTitle: Stakeholder Trust Erosion
Criticality: High
PossibleDamage: Loss of stakeholder trust and reputation damage
Category: Reputational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to communicate effectively with stakeholders can lead to misunderstandings, c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update stakeholders on progress and improvements", "2": "Address sta
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1258:
RiskId: 1510
ComplianceId: 2162
RiskTitle: Resistance to Change
Criticality: Medium
PossibleDamage: Misunderstandings and resistance from stakeholders
Category: Reputational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to communicate changes effectively can lead to stakeholder resistance, misun

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Hold special stakeholder meetings to address concerns", "2": "Provide detailed re
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1259:
RiskId: 1511
ComplianceId: 2163
RiskTitle: Ineffective Internal Audit for Impact Management Actions
Criticality: High
PossibleDamage: Failure to identify and address ineffective impact management actions
Category: Operational
RiskType: Current
BusinessImpact: All business units involved in impact management
RiskDescription: Inadequate internal audits may lead to ineffective tracking of impact management acti
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust audit schedule and ensure timely completion", "2": "Provide a
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1260:
RiskId: 1512

ComplianceId: 2164
RiskTitle: Inadequate Stakeholder Feedback Collection for Impact Management Actions
Criticality: Medium
PossibleDamage: Missing out on valuable insights for improving impact management actions
Category: Operational
RiskType: Current
BusinessImpact: All business units involved in impact management
RiskDescription: Insufficient stakeholder feedback collection may lead to overlooking critical perspectiv
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear feedback collection processes", "2": "Engage with diverse stakeho
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1261:
RiskId: 1513
ComplianceId: 2165
RiskTitle: Failure to Meet Impact Mitigation Targets
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, and negative environmental impact
Category: Environmental
RiskType: Residual
BusinessImpact: Potential harm to the environment and stakeholder trust
RiskDescription: If impact mitigation targets are not met, the company may face reputational damage,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement corrective actions to address missed targets", "2": "Enhance monitorin
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1262:
RiskId: 1514
ComplianceId: 2166
RiskTitle: Lack of Stakeholder Engagement
Criticality: High
PossibleDamage: Potential backlash from stakeholders and misalignment with organizational goals
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face challenges in decision-making and strategy implementati
RiskDescription: Failure to engage stakeholders may lead to decisions that do not align with stakehold
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly schedule stakeholder engagement sessions", "2": "Utilize diverse enga
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1263:
RiskId: 1515
ComplianceId: 2167
RiskTitle: Lack of Stakeholder Feedback Documentation
Criticality: Medium
PossibleDamage: Loss of valuable insights and inability to track stakeholder feedback over time

Category: Operational
RiskType: Inherent
BusinessImpact: Sustainability team may struggle to make informed decisions and develop effective st
RiskDescription: Failure to document stakeholder feedback may result in missed opportunities for impr
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Designate a team member for feedback documentation", "2": "Implement a centra
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1264:
RiskId: 1516
ComplianceId: 2168
RiskTitle: Failure to Conduct Due Diligence
Criticality: High
PossibleDamage: Regulatory fines, lawsuits, reputational damage, financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: Negative impact on operations, finances, and reputation
RiskDescription: Failure to conduct due diligence may result in unidentified risks and negative impacts
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear due diligence procedures", "2": "Regularly review and update risk
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1265:
RiskId: 1517
ComplianceId: 2169
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, leakage of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of trust, financial penalties
RiskDescription: Unauthorized access to sensitive information due to lack of RBAC implementation
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews", "2": "Continuous monitoring of access logs", "3": "Traini
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1266:
RiskId: 1518
ComplianceId: 2170
RiskTitle: Ineffective Incident Response Team
Criticality: High
PossibleDamage: Delayed or ineffective response to security incidents, leading to data breaches or se
Category: Operational
RiskType: Residual
BusinessImpact: IT, legal, communications departments
RiskDescription: Failure to establish an incident response team may result in delayed or ineffective res

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for the incident response team members", "2": "Ensure
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1267:
RiskId: 1519
ComplianceId: 2171
RiskTitle: Ineffective Incident Response Drills
Criticality: Medium
PossibleDamage: Unpreparedness and inefficiency in responding to security incidents, increasing the i
Category: Operational
RiskType: Residual
BusinessImpact: All organizational units
RiskDescription: Failure to conduct regular incident response drills may result in unpreparedness and i
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop realistic scenarios for the drills to simulate actual incidents", "2": "Evaluat
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1268:
RiskId: 1520

ComplianceId: 2172
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, loss of confidentiality
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, damage to reputation
RiskDescription: Unauthorized access to sensitive information can lead to data breaches and compron
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access rights", "2": "Implement multi-factor authentic
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1269:
RiskId: 1521
ComplianceId: 2173
RiskTitle: Outdated Access Rights
Criticality: Medium
PossibleDamage: Data breaches, loss of confidentiality
Category: Operational
RiskType: Current
BusinessImpact: Unauthorized access to sensitive information
RiskDescription: Outdated access rights can lead to unauthorized access and potential data breaches.
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regularly review access rights", "2": "Provide regular training on access control",
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1270:
RiskId: 1522
ComplianceId: 2174
RiskTitle: Inadequate Incident Response Team
Criticality: High
PossibleDamage: Delayed or ineffective response to security incidents, increased impact of breaches
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of services, data breaches, legal consequences
RiskDescription: Failure to establish a dedicated incident response team may lead to uncoordinated ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for IRT members", "2": "Continuous monitoring and upd
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1271:
RiskId: 1523
ComplianceId: 2175
RiskTitle: Inadequate Incident Response Drills
Criticality: Medium
PossibleDamage: Unpreparedness and inefficiency during security incidents, increased impact of brea

Category: Operational
RiskType: Residual
BusinessImpact: Disruption of services, data breaches, legal consequences
RiskDescription: Failure to conduct regular incident response drills may result in the IRT being unprepa
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Schedule and conduct bi-annual incident response drills", "2": "Analyze drill result
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1272:
RiskId: 1524
ComplianceId: 2176
RiskTitle: Failure to Conduct Timely Risk Assessments
Criticality: High
PossibleDamage: Data breaches and loss of sensitive information
Category: IT
RiskType: Inherent
BusinessImpact: All business units handling sensitive information
RiskDescription: Failure to conduct bi-annual risk assessments may lead to unidentified vulnerabilities
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated risk assessment tools", "2": "Provide regular training on risk
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 1273:
RiskId: 1525
ComplianceId: 2177
RiskTitle: Ineffective Incident Response Team
Criticality: High
PossibleDamage: Data breaches, operational disruptions, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, financial losses, regulatory fines
RiskDescription: Failure to respond promptly and effectively to security incidents can result in significar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for incident response team members", "2": "Simulated incident re
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1274:
RiskId: 1526
ComplianceId: 2178
RiskTitle: Incomplete Incident Response Plan
Criticality: Medium
PossibleDamage: Confusion, delays in incident resolution, inadequate response to security incidents
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, data breaches, reputational damage
RiskDescription: An incomplete or outdated incident response plan can lead to inefficiencies and inade

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update of incident response plan", "2": "Integration of incident
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1275:
RiskId: 1527
ComplianceId: 2179
RiskTitle: Non-compliance with ITU Recommendations
Criticality: High
PossibleDamage: Potential security vulnerabilities and non-compliance issues
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to comply with ITU Recommendations can lead to security vulnerabilities, data
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of compliance status", "2": "Immediate remediation of non-com
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1276:
RiskId: 1528

ComplianceId: 2180
RiskTitle: Non-Compliance Risk
Criticality: High
PossibleDamage: Potential regulatory penalties and service disruptions
Category: Compliance
RiskType: Residual
BusinessImpact: All business units would be impacted by potential penalties
RiskDescription: Failure to monitor compliance could lead to non-compliance with ITU Recommendatio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for Compliance Officer on monitoring procedures", "2": "Automate
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1277:
RiskId: 1529
ComplianceId: 2181
RiskTitle: Reporting Accuracy Risk
Criticality: Medium
PossibleDamage: Misinformed decisions due to inaccurate reports
Category: Compliance
RiskType: Residual
BusinessImpact: All business units would be impacted by misinformed decisions
RiskDescription: Failure to generate accurate compliance reports could lead to misinformed decisions
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regular review of report generation process for accuracy", "2": "Implement data v
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1278:
RiskId: 1530
ComplianceId: 2182
RiskTitle: Data Breach Due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive information, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of customer trust and legal consequences
RiskDescription: Unauthorized access to sensitive information could lead to data breaches and compro
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access rights reviews", "2": "Training on access control best practices", "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1279:
RiskId: 1531
ComplianceId: 2183
RiskTitle: Unauthorized Access Due to Outdated Access Rights
Criticality: Medium
PossibleDamage: Data breaches, loss of sensitive information

Category: IT
RiskType: Residual
BusinessImpact: Potential loss of data integrity and confidentiality
RiskDescription: Outdated access rights could result in unauthorized access to sensitive information, le
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated access rights review tools", "2": "Training on access rights manageme
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1280:
RiskId: 1532
ComplianceId: 2184
RiskTitle: Ineffective Incident Response Team
Criticality: High
PossibleDamage: Delayed incident response, inadequate incident management, increased impact of s
Category: Operational
RiskType: Current
BusinessImpact: All business units handling information systems
RiskDescription: Failure to establish an incident response team may lead to delayed or ineffective incid
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for the incident response team members", "2": "Docume
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1281:
RiskId: 1533
ComplianceId: 2185
RiskTitle: Undefined Incident Reporting Procedures
Criticality: Medium
PossibleDamage: Delays in incident identification and response, increased impact and potential data b
Category: Operational
RiskType: Current
BusinessImpact: All business units handling information systems
RiskDescription: Lack of defined incident reporting procedures may result in delays in incident identifica
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular communication and training on incident reporting procedures", "2": "Perio
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1282:
RiskId: 1534
ComplianceId: 2186
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Financial loss, reputational damage, legal implications
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of customer trust and business continuity
RiskDescription: Unauthorized access to sensitive data due to improper data classification and handlin

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for sensitive data", "2": "Regularly review and update data
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1283:
RiskId: 1535
ComplianceId: 2187
RiskTitle: Delayed Investigation Initiation
Criticality: High
PossibleDamage: Loss of crucial evidence and compromised investigation integrity
Category: Operational
RiskType: Current
BusinessImpact: Delayed investigations may lead to unresolved policy violations and potential legal co
RiskDescription: Failure to initiate investigations within 48 hours may result in loss of key evidence, wit
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear escalation procedures for delayed investigations", "2": "Provide tra
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1284:
RiskId: 1536

ComplianceId: 2188
RiskTitle: Inconsistent Investigation Procedures
Criticality: Medium
PossibleDamage: Incomplete or biased investigation findings
Category: Operational
RiskType: Current
BusinessImpact: Inconsistent investigation procedures may lead to incomplete or biased findings, resu
RiskDescription: Failure to utilize standardized investigation forms and protocols may result in inconsis
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide training on the proper use of standardized forms and protocols", "2": "Reg
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1285:
RiskId: 1537
ComplianceId: 2189
RiskTitle: Data Breach via Unsecured Connection
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Unauthorized access to organizational data due to lack of secure connection usage
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly update VPN software", "2": "Implement multi-factor authentication for V
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1286:
RiskId: 1538
ComplianceId: 2190
RiskTitle: Unauthorized Device Access
Criticality: Medium
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, potential legal consequences
RiskDescription: Unauthorized access to organizational data due to lack of device password protection
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enforce strong password policies for devices", "2": "Implement device encryption
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1287:
RiskId: 1539
ComplianceId: 2191
RiskTitle: Delayed Reporting of Security Events
Criticality: High
PossibleDamage: Increased severity of security incidents and prolonged exposure to threats

Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, data breaches, and reputational damage
RiskDescription: Failure to report security events within the specified timeframe may result in escalated
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reporting reminders", "2": "Enhance incident reporting train
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1288:
RiskId: 1540
ComplianceId: 2192
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, physical security threats
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, compromised physical security
RiskDescription: Unauthorized individuals gaining access to secure areas can lead to theft of physical
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews to ensure access is still necessary", "2": "Implement two-
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1289:
RiskId: 1541
ComplianceId: 2193
RiskTitle: Delayed Access Review Risk
Criticality: Medium
PossibleDamage: Prolonged unauthorized access, security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of unauthorized access, potential security breaches
RiskDescription: Delayed access reviews can allow unauthorized individuals to exploit the system and
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate access request notifications for timely review", "2": "Implement escalati
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1290:
RiskId: 1542
ComplianceId: 2194
RiskTitle: Unauthorized Access to Production Environments
Criticality: High
PossibleDamage: Data breaches, system disruptions, loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of production operations, financial losses, reputational damage
RiskDescription: Unauthorized access to production environments can lead to data breaches, system

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews to ensure access rights are up to date", "2": "Monitoring a
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1291:
RiskId: 1543
ComplianceId: 2195
RiskTitle: Late Submission of Change Requests
Criticality: High
PossibleDamage: Delayed implementation of critical changes
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions and potential financial losses
RiskDescription: Late submission of change requests can lead to rushed approvals or delays in implem
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear submission deadlines and consequences for late submissions", "2
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1292:
RiskId: 1544

ComplianceId: 2196
RiskTitle: Inadequate Evaluation of Change Requests
Criticality: Critical
PossibleDamage: System failures, data breaches, or service disruptions
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, reputational damage, and legal implications
RiskDescription: Approval of changes without proper evaluation could result in system failures, data br
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear evaluation criteria for change requests", "2": "Regular training and
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1293:
RiskId: 1545
ComplianceId: 2197
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, compromise of system integrity
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, damage to system integrity
RiskDescription: Risk of unauthorized individuals gaining access to sensitive information during audit te
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular access reviews to ensure access is revoked post-audit", "2": "Multi-factor
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1294:
RiskId: 1546
ComplianceId: 2198
RiskTitle: Access Logs Maintenance Risk
Criticality: Medium
PossibleDamage: Lack of accountability, inability to trace unauthorized actions
Category: Operational
RiskType: Residual
BusinessImpact: Inability to track auditor actions, potential unauthorized activities going unnoticed
RiskDescription: Risk of not maintaining access logs for auditors during testing, leading to lack of acco
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review of access logs for any suspicious activity", "2": "Implementing auto
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1295:
RiskId: 1547
ComplianceId: 2199
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches and loss of confidentiality

Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive information, reputational damage, financial losses.
RiskDescription: Risk of unauthorized access to sensitive telecommunications information leading to da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access control lists", "2": "Implement multi-factor aut
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1296:
RiskId: 1548
ComplianceId: 2200
RiskTitle: Encryption Vulnerability Risk
Criticality: High
PossibleDamage: Data breaches and loss of confidentiality
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive information, reputational damage, financial losses.
RiskDescription: Risk of exposure of sensitive telecommunications information due to lack of encryptio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption protocols for data in transit and at rest", "2": "Regularly upd
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1297:
RiskId: 1549
ComplianceId: 2201
RiskTitle: Data Integrity Compromise
Criticality: High
PossibleDamage: Data corruption, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, compromised network security
RiskDescription: Failure to implement checksums and digital signatures may lead to data corruption du
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and maintain checksum and digital signature algorithms", "2": "I
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1298:
RiskId: 1550
ComplianceId: 2202
RiskTitle: Data Integrity Validation Failure
Criticality: Medium
PossibleDamage: Inaccurate information, system vulnerabilities
Category: IT
RiskType: Residual
BusinessImpact: Potential data inaccuracies, system vulnerabilities
RiskDescription: Failure to validate data integrity after system updates or installations may lead to inac

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Perform regular integrity checks after system updates or installations", "2": "Imple
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1299:
RiskId: 1551
ComplianceId: 2203
RiskTitle: Disruption of Essential Communications
Criticality: High
PossibleDamage: Loss of critical information and services
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, potential safety risks
RiskDescription: Failure to prioritize essential communications during emergencies can lead to service
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and test the business continuity plan", "2": "Ensure clear commu
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1300:
RiskId: 1552

ComplianceId: 2204
RiskTitle: Inadequate Response During Emergencies
Criticality: Medium
PossibleDamage: Ineffective business continuity plan
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, potential financial losses
RiskDescription: Failure to test and update the business continuity plan annually can result in an inade
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly schedule and conduct annual tests of the business continuity plan", "2":
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1301:
RiskId: 1553
ComplianceId: 2205
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data loss, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Failure to identify and address security vulnerabilities may lead to unauthorized acces
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement encryption measures for sensitive data", "2": "Regularly update securit
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1302:
RiskId: 1554
ComplianceId: 2206
RiskTitle: Change-Related Risk
Criticality: Medium
PossibleDamage: Exposure to new vulnerabilities and threats
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, potential data breaches
RiskDescription: Failure to assess risks associated with changes in the environment may result in unac
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement change control procedures", "2": "Conduct impact analysis for changes
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1303:
RiskId: 1555
ComplianceId: 2207
RiskTitle: Ineffective Incident Response
Criticality: High
PossibleDamage: Prolonged downtime, data breaches, financial losses

Category: Operational
RiskType: Residual
BusinessImpact: Disruption of telecommunications operations, loss of sensitive data
RiskDescription: Failure to respond effectively to incidents can lead to prolonged downtime, data breac
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the incident response plan based on lessons learne
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1304:
RiskId: 1556
ComplianceId: 2208
RiskTitle: Outdated Incident Response Plan
Criticality: Medium
PossibleDamage: Ineffective incident management
Category: Operational
RiskType: Residual
BusinessImpact: Inability to effectively respond to incidents
RiskDescription: Failure to review and test the incident response plan may lead to outdated procedures
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Schedule regular reviews and tests in advance to ensure compliance", "2": "Docu
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 1305:
RiskId: 1557
ComplianceId: 2209
RiskTitle: Outdated Normative References
Criticality: High
PossibleDamage: Non-compliance with industry standards, increased security risks, potential data bre
Category: Operational
RiskType: Residual
BusinessImpact: Information Security Management
RiskDescription: Failure to update normative references may result in outdated practices, non-compli
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on the importance of updating references", "2": "Automated remi
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1306:
RiskId: 1558
ComplianceId: 2210
RiskTitle: Misuse of Undefined Terms
Criticality: High
PossibleDamage: Misinterpretation of organizational documents, leading to errors or non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: Increased risk of errors in policy documents and potential compliance violations
RiskDescription: Failure to define and approve new terms and abbreviations may result in inconsistent

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training on the correct usage of approved terms and abbreviations", "2": "
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1307:
RiskId: 1559
ComplianceId: 2211
RiskTitle: Data Breach due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Financial loss, legal implications
RiskDescription: Unauthorized access to sensitive information can lead to data breaches and compron
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews", "2": "Training on RBAC implementation", "3": "Continuo
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1308:
RiskId: 1560

ComplianceId: 2212
RiskTitle: Ineffective Incident Response Team
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to respond effectively to security incidents due to lack of established incident r
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for the incident response team", "2": "Continuous monit
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1309:
RiskId: 1561
ComplianceId: 2213
RiskTitle: Delayed Incident Reporting
Criticality: Medium
PossibleDamage: Prolonged exposure to security threats, increased impact on operations
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Incidents not reported immediately upon detection leading to prolonged exposure to s
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Continuous training on incident detection and reporting", "2": "Establish clear repo
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1310:
RiskId: 1562
ComplianceId: 2214
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of sensitive data and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: All business units handling sensitive data
RiskDescription: Risk of unauthorized access to sensitive data leading to data breaches and potential l
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for data protection", "2": "Regularly audit data access contr
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1311:
RiskId: 1563
ComplianceId: 2215
RiskTitle: Data Protection Vulnerability Risk
Criticality: Medium
PossibleDamage: Exposure of sensitive data due to ineffective data protection measures

Category: Operational
RiskType: Current
BusinessImpact: All business units handling sensitive data
RiskDescription: Risk of data protection vulnerabilities due to outdated or ineffective measures, leading
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update data protection measures", "2": "Implement recomm
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1312:
RiskId: 1564
ComplianceId: 2216
RiskTitle: Unauthorized Access to Telecommunications Systems
Criticality: High
PossibleDamage: Data breaches, system compromise, loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Unauthorized access to telecommunications systems can lead to data breaches, syst
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews", "2": "Monitoring access logs", "3": "Implementing multi-f
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1313:
RiskId: 1565
ComplianceId: 2217
RiskTitle: Ineffective Incident Response
Criticality: High
PossibleDamage: Data breaches, service disruptions, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of services, loss of customer trust
RiskDescription: Failure to respond effectively to incidents may lead to prolonged service disruptions a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for incident response team members", "2": "Continuous
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1314:
RiskId: 1566
ComplianceId: 2218
RiskTitle: Outdated Incident Response Plan
Criticality: Medium
PossibleDamage: Ineffective responses during incidents
Category: Operational
RiskType: Residual
BusinessImpact: Service disruptions, financial losses
RiskDescription: Failure to update and test the incident response plan may result in delays and errors i

RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly scheduled testing and simulation exercises", "2": "Immediate updates fo
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1315:
RiskId: 1567
ComplianceId: 2219
RiskTitle: Malware Infection Risk
Criticality: High
PossibleDamage: Data breaches, system downtime, financial losses
Category: IT
RiskType: Residual
BusinessImpact: IT Operations, Data Security
RiskDescription: Failure to conduct weekly malware scans may result in undetected malware infections
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update malware definitions", "2": "Implement real-time monitoring for im
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1316:
RiskId: 1568

ComplianceId: 2220
RiskTitle: Delayed Malware Protection Updates Risk
Criticality: Medium
PossibleDamage: Systems vulnerable to new malware threats, potential data breaches
Category: IT
RiskType: Residual
BusinessImpact: IT Operations, Data Security
RiskDescription: Failure to apply immediate malware protection updates may leave systems vulnerable
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish automated update processes for immediate deployment", "2": "Regularly
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1317:
RiskId: 1569
ComplianceId: 2221
RiskTitle: Confusion in Roles and Responsibilities
Criticality: High
PossibleDamage: Unauthorized access, data breaches, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Potential security breaches impacting all business units
RiskDescription: Lack of clarity in roles and responsibilities may lead to confusion, errors, and security
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training sessions to reinforce roles and responsibilities", "2": "Periodic rev
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1318:
RiskId: 1570
ComplianceId: 2222
RiskTitle: Insufficient Information Security Training
Criticality: High
PossibleDamage: Data breaches, unauthorized access, and non-compliance penalties
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Lack of understanding of information security policies and procedures leading to incre
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of training completion status", "2": "Provide refresher courses
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1319:
RiskId: 1571
ComplianceId: 2223
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, compliance violations

Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, legal consequences, damage to reputation
RiskDescription: The risk of unauthorized access to information systems leading to potential data brea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews to ensure access rights are up to date", "2": "Implement r
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1320:
RiskId: 1572
ComplianceId: 2224
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses and damage to reputation.
RiskDescription: Unauthorized access could lead to data breaches and misuse of resources, resulting
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly monitor access logs for an
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1321:
RiskId: 1573
ComplianceId: 2225
RiskTitle: Role Misalignment Risk
Criticality: Medium
PossibleDamage: Unauthorized actions, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Potential operational disruptions and compliance penalties.
RiskDescription: Failure to adjust access rights based on role changes could lead to unauthorized acti
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate role-based access reviews", "2": "Implement regular role change audits
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1322:
RiskId: 1574
ComplianceId: 2226
RiskTitle: Data Breach Due to Supplier Non-Compliance
Criticality: High
PossibleDamage: Data breaches, legal consequences, loss of customer trust
Category: Compliance
RiskType: Current
BusinessImpact: Financial losses, reputational damage, regulatory fines
RiskDescription: Failure of suppliers to comply with data protection clauses in agreements may result i

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of supplier compliance", "2": "Immediate termination of agreer
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1323:
RiskId: 1575
ComplianceId: 2227
RiskTitle: Delayed Incident Reporting
Criticality: High
PossibleDamage: Prolonged exposure of customer data, reputational damage, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of customer trust, financial penalties, legal consequences
RiskDescription: Failure to report incidents promptly may result in extended exposure of sensitive cust
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated incident reporting tools", "2": "Provide regular incident repo
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1324:
RiskId: 1576

ComplianceId: 2228
RiskTitle: Failure to Escalate Incidents
Criticality: Medium
PossibleDamage: Prolonged downtime, increased impact on customers, financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: Customer dissatisfaction, financial repercussions, operational disruptions
RiskDescription: Lack of timely escalation of incidents beyond defined service levels may result in exte
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear escalation criteria and communication channels", "2": "Regularly re
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1325:
RiskId: 1577
ComplianceId: 2229
RiskTitle: Inadequate Documentation Risk
Criticality: High
PossibleDamage: Confusion, errors, and security breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling sensitive information
RiskDescription: Failure to document and maintain operating procedures can result in unauthorized ac
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training on procedure documentation", "2": "Automated reminders for anr
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1326:
RiskId: 1578
ComplianceId: 2230
RiskTitle: Ineffective Response to Spam Incidents
Criticality: High
PossibleDamage: Increased spam incidents, reputation damage, legal implications
Category: Operational
RiskType: Current
BusinessImpact: Disruption of services, legal consequences, damage to reputation
RiskDescription: Failure to effectively respond to spam incidents can lead to an increase in spam, pote
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update spam response policies", "2": "Provide ongoing train
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1327:
RiskId: 1579
ComplianceId: 2231
RiskTitle: Outdated Spam Response Policies
Criticality: Medium
PossibleDamage: Ineffective response to evolving spam threats, potential security breaches

Category: Operational
RiskType: Current
BusinessImpact: Increased spam incidents, security vulnerabilities
RiskDescription: Failure to review spam response policies regularly may result in outdated procedures
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Schedule regular policy review meetings", "2": "Document policy review outcomes
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1328:
RiskId: 1580
ComplianceId: 2232
RiskTitle: Impact of DoS/DDoS Attacks on Telecommunications Services
Criticality: High
PossibleDamage: Prolonged service disruptions, data breaches, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of services, loss of customer trust, financial losses
RiskDescription: DoS/DDoS attacks can lead to service downtime, data breaches, and reputational dar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for the Network Security Team on response procedures
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1329:
RiskId: 1581
ComplianceId: 2233
RiskTitle: Network Vulnerability to Malicious Traffic
Criticality: High
PossibleDamage: Network downtime, data breaches, and compromised network resources
Category: IT
RiskType: Inherent
BusinessImpact: Network security, data integrity, and operational continuity would be impacted.
RiskDescription: Failure to implement packet filtering protocols may expose the network to malicious tr
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and maintain intrusion detection systems and firewalls", "2": "Im
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 1330:
RiskId: 1582
ComplianceId: 2234
RiskTitle: DDoS Attack Impact on Network Availability
Criticality: High
PossibleDamage: Network downtime, service unavailability, and financial losses
Category: IT
RiskType: Inherent
BusinessImpact: Network availability, service continuity, and financial stability would be impacted.
RiskDescription: Failure to detect and mitigate DDoS attacks promptly may lead to prolonged network

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement DDoS mitigation tools and services", "2": "Establish incident response
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1331:
RiskId: 1583
ComplianceId: 2235
RiskTitle: Network Service Disruption
Criticality: High
PossibleDamage: Disruption of network services, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of customer trust, financial losses
RiskDescription: Failure to suspend services promptly may lead to prolonged network downtime and fi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Isolate affected customer traffic", "2": "Notify customer of suspension and provide
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1332:
RiskId: 1584

ComplianceId: 2236
RiskTitle: Customer Dissatisfaction
Criticality: Medium
PossibleDamage: Customer complaints, legal disputes
Category: Operational
RiskType: Current
BusinessImpact: Potential damage to the organization's reputation, legal consequences
RiskDescription: Inadequate customer notification may result in customer dissatisfaction, complaints, a
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide clear and detailed reasons for suspension", "2": "Offer guidance on resolv
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1333:
RiskId: 1585
ComplianceId: 2237
RiskTitle: Breach of Confidentiality Agreements
Criticality: High
PossibleDamage: Legal actions, financial penalties, loss of trust from stakeholders, damage to reputati
Category: Operational
RiskType: Current
BusinessImpact: Legal and financial implications, reputational damage.
RiskDescription: Failure to comply with confidentiality agreements may result in unauthorized disclosur
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular monitoring of agreement compliance", "2": "Immediate response to suspe

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1334:

RiskId: 1586

ComplianceId: 2238

RiskTitle: Inadequate Review of Confidentiality Agreements

Criticality: Medium

PossibleDamage: Failure to update agreements may result in ineffective protection of sensitive commu

Category: Operational

RiskType: Current

BusinessImpact: Legal implications, reputational damage.

RiskDescription: Lack of regular review and updates to confidentiality agreements may render them ine

RiskLikelihood: 7

RiskImpact: 6

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear review timelines for agreements", "2": "Automate reminders for ag

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1335:

RiskId: 1587

ComplianceId: 2239

RiskTitle: Legal Penalties for Non-Compliance

Criticality: High

PossibleDamage: Financial penalties, reputational damage

Category: Compliance
RiskType: Current
BusinessImpact: Legal fines, loss of customer trust
RiskDescription: Failure to establish data retention periods can result in non-compliance with legal requ
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure compliance", "2": "Training for data management team c
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1336:
RiskId: 1588
ComplianceId: 2240
RiskTitle: Data Breaches Due to Retained Data
Criticality: High
PossibleDamage: Loss of customer trust, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Data breaches, legal penalties
RiskDescription: Failure to delete data promptly can result in unauthorized access to sensitive informat
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing of data deletion processes", "2": "Encryption of retained data", "3"
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1337:
RiskId: 1589
ComplianceId: 2241
RiskTitle: Miscommunication during emergencies
Criticality: High
PossibleDamage: Delayed response, increased risk to individuals
Category: Operational
RiskType: Residual
BusinessImpact: Potential harm to individuals and property
RiskDescription: Failure to activate communication protocols immediately can lead to confusion, delays
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for emergency response team", "2": "Regular testing of
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 1338:
RiskId: 1590
ComplianceId: 2242
RiskTitle: Inefficient communication management
Criticality: Medium
PossibleDamage: Delays in emergency response, potential confusion
Category: Operational
RiskType: Residual
BusinessImpact: Impact on emergency response efficiency
RiskDescription: Failure to utilize communication management systems effectively can lead to delays i

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on communication systems", "2": "Regular maintenance and upd
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1339:
RiskId: 1591
ComplianceId: 2243
RiskTitle: Miscommunication during Emergencies
Criticality: High
PossibleDamage: Delayed response, confusion, increased risks
Category: Operational
RiskType: Current
BusinessImpact: Legal, Compliance
RiskDescription: Failure to establish communication agreements with external agencies may result in r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on communication protocols", "2": "Simulated emergenc
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1340:
RiskId: 1592

ComplianceId: 2244
RiskTitle: Inadequate Incident Coordination
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, loss of customer trust
RiskDescription: Failure to coordinate incident response effectively leading to increased severity of inci
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication protocols in advance", "2": "Regularly train person
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1341:
RiskId: 1593
ComplianceId: 2245
RiskTitle: Ineffective Communication Channels
Criticality: Medium
PossibleDamage: Miscommunication, delays in incident response, ineffective collaboration
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, regulatory fines, reputational damage
RiskDescription: Failure to utilize established communication channels leading to delays, errors, and in
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly review and update communication channels", "2": "Provide training on c

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 1342:

RiskId: 1594

ComplianceId: 2246

RiskTitle: Unauthorized Access to Facilities

Criticality: High

PossibleDamage: Data breaches, service disruption, physical damage

Category: Operational

RiskType: Current

BusinessImpact: Loss of sensitive data, operational downtime, reputational damage

RiskDescription: Unauthorized individuals gaining access to critical infrastructure and data centers

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement access control measures", "2": "Regularly review and update security p

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1343:

RiskId: 1595

ComplianceId: 2247

RiskTitle: Unauthorized Access Risk

Criticality: High

PossibleDamage: Unauthorized access to sensitive data, potential data breaches

Category: Operational
RiskType: Current
BusinessImpact: Potential compromise of sensitive data and operational disruptions
RiskDescription: Risk of unauthorized individuals gaining access to telecommunications operation roor
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff on visitor management procedures", "2": "Regular audits
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1344:
RiskId: 1596
ComplianceId: 2248
RiskTitle: Outdated Visitor Logs Risk
Criticality: Medium
PossibleDamage: Outdated visitor logs leading to security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of unauthorized access due to outdated logs
RiskDescription: Risk of security vulnerabilities and potential unauthorized access due to outdated visit
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated alerts for real-time log updates", "2": "Regular training on log maintena
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1345:
RiskId: 1597
ComplianceId: 2249
RiskTitle: Data Breach Due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive information, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal implications
RiskDescription: Unauthorized access to sensitive information can lead to data breaches and significar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update access control systems", "2": "Implement multi-factor authentica
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1346:
RiskId: 1598
ComplianceId: 2250
RiskTitle: Security Breach Due to Unidentified Vulnerabilities
Criticality: Medium
PossibleDamage: Loss of sensitive information, operational disruptions
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions, financial losses
RiskDescription: Failure to identify and address security vulnerabilities can lead to security breaches ar

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a schedule for regular security assessments", "2": "Train staff on secu
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1347:
RiskId: 1599
ComplianceId: 2251
RiskTitle: Security Breach Due to Lack of Monitoring
Criticality: High
PossibleDamage: Data loss, physical harm, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, legal implications
RiskDescription: Failure to monitor surveillance systems may result in delayed detection of security inc
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and analysis of surveillance data", "2": "Immediate response p
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1348:
RiskId: 1600

ComplianceId: 2252
RiskTitle: Risk of Facility Damage from Environmental Threats
Criticality: High
PossibleDamage: Severe damage to facilities, disruption of operations
Category: Environmental
RiskType: Current
BusinessImpact: Facility damage, operational disruptions
RiskDescription: Potential for facilities to be severely damaged by environmental threats leading to ope
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement disaster recovery plans", "2": "Enhance environmental controls", "3": "I
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1349:
RiskId: 1601
ComplianceId: 2253
RiskTitle: Risk of Secondary Damage Post-Environmental Event
Criticality: Medium
PossibleDamage: Further damage due to lack of post-event assessment and mitigation
Category: Environmental
RiskType: Current
BusinessImpact: Further damage to facilities, prolonged operational disruptions
RiskDescription: Failure to conduct post-event risk assessments could lead to secondary damage and
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Conduct immediate assessment post-event", "2": "Implement corrective actions p
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1350:
RiskId: 1602
ComplianceId: 2254
RiskTitle: HVAC System Failure
Criticality: High
PossibleDamage: Risk of equipment damage and service disruption
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of critical services and potential financial impact
RiskDescription: Failure of HVAC systems can lead to equipment overheating, humidity damage, and s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular maintenance of HVAC systems", "2": "Temperature and humidity monitor
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1351:
RiskId: 1603
ComplianceId: 2255
RiskTitle: Fire Hazard
Criticality: High
PossibleDamage: Risk of equipment damage, data loss, and harm to personnel in case of fire

Category: Operational
RiskType: Inherent
BusinessImpact: Loss of critical services, potential harm to personnel, and financial impact
RiskDescription: Fire incidents can lead to equipment damage, data loss, and potential harm to person
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular inspection and testing of fire suppression systems", "2": "Employee traini
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1352:
RiskId: 1604
ComplianceId: 2256
RiskTitle: Unauthorized Access to Telecommunications Equipment Rooms
Criticality: High
PossibleDamage: Data breaches, equipment damage, service disruption
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial losses, reputational damage
RiskDescription: Unauthorized access to telecommunications equipment rooms can result in data brea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits and access logs to monitor access", "2": "Training sessions for per
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1353:
RiskId: 1605
ComplianceId: 2257
RiskTitle: Undetected Unauthorized Access to Telecommunications Equipment Rooms
Criticality: Medium
PossibleDamage: Security breaches, data loss, compromised security
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, compromised security, reputational damage
RiskDescription: Failure to conduct regular audits and maintain access logs can result in undetected u
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training for personnel on audit procedures", "2": "Automated audit tools fo
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 1354:
RiskId: 1606
ComplianceId: 2258
RiskTitle: Earthquake Structural Failure Risk
Criticality: High
PossibleDamage: Structural collapse leading to injury or loss of critical infrastructure.
Category: Operational
RiskType: Current
BusinessImpact: Construction delays, financial losses, and reputational damage.
RiskDescription: The risk of structural failure in isolated operating areas during seismic events due to i

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Use seismic-resistant materials and construction techniques", "2": "Regular struct
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1355:
RiskId: 1607
ComplianceId: 2259
RiskTitle: Fire Outbreak Risk
Criticality: High
PossibleDamage: Fire outbreaks leading to property damage, data loss, and operational disruptions.
Category: Operational
RiskType: Current
BusinessImpact: Property damage, data loss, business interruptions, and reputational harm.
RiskDescription: The risk of fire incidents in isolated operating areas due to the absence of automatic f
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Install automatic fire detection and suppression systems", "2": "Regular maintena
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1356:
RiskId: 1608

ComplianceId: 2260
RiskTitle: Failure to Detect Fire Incident
Criticality: High
PossibleDamage: Equipment damage, safety hazards, potential injuries
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Failure to detect a fire incident in an isolated operating area could result in equipment
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular fire safety drills and training for employees", "2": "Implementation of auto
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1357:
RiskId: 1609
ComplianceId: 2261
RiskTitle: Delay in Incident Response
Criticality: Medium
PossibleDamage: Extended downtime, safety risks, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, potential safety hazards, reputational damage
RiskDescription: A delay in responding to incidents detected in isolated operating areas due to failure i
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear escalation procedures for alerts", "2": "Regular training for operati

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1358:

RiskId: 1610

ComplianceId: 2262

RiskTitle: Data Breach Due to Inadequate Security Configurations

Criticality: High

PossibleDamage: Data loss, reputational damage, legal consequences

Category: IT

RiskType: Residual

BusinessImpact: Loss of sensitive data, financial penalties, damage to reputation

RiskDescription: Inadequate security configurations may lead to vulnerabilities that could be exploited

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update security configurations", "2": "Implement multi-factor authenticat

CreatedAt: 2025-10-25 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1359:

RiskId: 1611

ComplianceId: 2263

RiskTitle: Failure to Detect Security Incidents on User Endpoint Devices

Criticality: Medium

PossibleDamage: Data breaches, malware infections, operational disruptions

Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, system downtime, reputational damage
RiskDescription: Inadequate monitoring of user endpoint devices may result in undetected security inci
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated alerts for security incidents", "2": "Regularly review monitor
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1360:
RiskId: 1612
ComplianceId: 2264
RiskTitle: Unauthorized Access to Sensitive Data
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Unauthorized access to sensitive data by unauthorized personnel leading to data brea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access control lists", "2": "Implement multi-factor aut
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 1361:
RiskId: 1613
ComplianceId: 2265
RiskTitle: Outdated Access Rights
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Outdated access rights for privileged accounts leading to unauthorized access, poten
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate access rights review process", "2": "Implement regular training for Acce
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1362:
RiskId: 1614
ComplianceId: 2266
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, loss of confidentiality, legal repercussions
Category: Compliance
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties, reputational damage
RiskDescription: Unauthorized access to sensitive information can lead to data breaches, loss of confi

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access controls", "2": "Regularly review and update access
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1363:
RiskId: 1615
ComplianceId: 2267
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, potential data breaches
Category: IT
RiskType: Inherent
BusinessImpact: All business units would be impacted by unauthorized access
RiskDescription: Risk of unauthorized individuals gaining access to sensitive data through compromise
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Regularly review access logs for suspi
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1364:
RiskId: 1616

ComplianceId: 2268
RiskTitle: Malware Infection Risk
Criticality: High
PossibleDamage: Data breaches, system downtime, loss of sensitive information
Category: IT
RiskType: Inherent
BusinessImpact: Disruption of business operations, financial losses
RiskDescription: Failure to implement anti-malware solutions may lead to malware infections comprom
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update anti-malware definitions", "2": "Conduct regular malware scans
CreatedAt: 2025-10-25 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1365:
RiskId: 1311
ComplianceId: None
RiskTitle: Non-Compliance with Capital Adequacy Standards ai
Criticality: Critical
PossibleDamage: Potential financial insolvency and regulatory fines.
Category: Regulatory
RiskType: Current
BusinessImpact: High
RiskDescription: Risk associated with failure to maintain adequate capital reserves.
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 75.5
RiskMultiplierX: 1.2
RiskMultiplierY: 1.2

RiskPriority: Critical
RiskMitigation: "{\"1\": \"Increase capital reserves and perform quarterly recalculations.\"} Excess mitiga
CreatedAt: 2025-10-24 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1366:
RiskId: 1312
ComplianceId: None
RiskTitle: Non-Compliance with Capital Adequacy Standards ai
Criticality: Critical
PossibleDamage: Potential financial insolvency and regulatory fines.
Category: Regulatory
RiskType: Inherent
BusinessImpact: High financial impact due to potential insolvency and significant regulatory fines, whic
RiskDescription: Risk associated with failure to maintain adequate capital reserves.
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 75.5
RiskMultiplierX: 1.2
RiskMultiplierY: 1.2
RiskPriority: High
RiskMitigation: "{\"1\": \"Increase capital reserves and perform quarterly recalculations.\"} Excess mitiga
CreatedAt: 2025-10-24 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1367:
RiskId: 1313
ComplianceId: None
RiskTitle: Non-Compliance with Capital Adequacy Standards ai
Criticality: Critical
PossibleDamage: Risk Priority: High

Category: Regulatory
RiskType: Inherent
BusinessImpact: Significant financial penalties and potential loss of operational licenses due to non-co
RiskDescription: Risk associated with failure to maintain adequate capital reserves.
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 75.5
RiskMultiplierX: 1.2
RiskMultiplierY: 1.3
RiskPriority: High
RiskMitigation: "{\"1\": \"Increase capital reserves and perform quarterly recalculations.\"} Excess mitiga
CreatedAt: 2025-10-24 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1368:
RiskId: 1314
ComplianceId: None
RiskTitle: Non-Compliance with Capital Adequacy Standards ai
Criticality: Critical
PossibleDamage: Risk Priority: High
Category: Regulatory
RiskType: Inherent
BusinessImpact: Significant financial penalties and operational disruptions due to non-compliance with
RiskDescription: Risk associated with failure to maintain adequate capital reserves.
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 75.5
RiskMultiplierX: 1.2
RiskMultiplierY: 1.3
RiskPriority: High
RiskMitigation: "{\"1\": \"Increase capital reserves and perform quarterly recalculations.\"} Excess mitiga
CreatedAt: 2025-10-24 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1369:
RiskId: 1315
ComplianceId: None
RiskTitle: Non-Compliance with Capital Adequacy Standards
Criticality: Critical
PossibleDamage: Potential financial insolvency and regulatory fines.
Category: Regulatory
RiskType: Current
BusinessImpact: High
RiskDescription: Risk associated with failure to maintain adequate capital reserves.
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 75.5
RiskMultiplierX: 1.2
RiskMultiplierY: 1.3
RiskPriority: Critical
RiskMitigation: "{\"1\": \"Increase capital reserves and perform quarterly recalculations.\"} Excess mitiga
CreatedAt: 2025-10-24 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1370:
RiskId: 1316
ComplianceId: None
RiskTitle: Non-Compliance with Capital Adequacy Standards
Criticality: Critical
PossibleDamage: Potential financial insolvency and regulatory fines.
Category: Regulatory
RiskType: Inherent
BusinessImpact: High financial impact due to potential insolvency and significant regulatory fines, whic
RiskDescription: Risk associated with failure to maintain adequate capital reserves.

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 75.5
RiskMultiplierX: 1.2
RiskMultiplierY: 1.2
RiskPriority: High
RiskMitigation: "{\"1\": \"Increase capital reserves and perform quarterly recalculations.\"} Excess mitiga
CreatedAt: 2025-10-24 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1371:
RiskId: 1309
ComplianceId: None
RiskTitle: security network brached
Criticality: Critical
PossibleDamage: The security breach could lead to unauthorized access to sensitive customer data, fi
Category: People Risk
RiskType: Current
BusinessImpact: Customer Impact
RiskDescription: The security breach occurred due to unauthorized access by hackers, leading to pote
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 6.48
RiskMultiplierX: 0.3
RiskMultiplierY: 0.3
RiskPriority: High
RiskMitigation: Implement multi-factor authentication for all system access to prevent unauthorized log
CreatedAt: 2025-10-22 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1372:
RiskId: 1310

ComplianceId: 11
RiskTitle: security network brached
Criticality: Critical
PossibleDamage: The security breach could lead to unauthorized access to sensitive customer data, fi
Category: People Risk
RiskType: Current
BusinessImpact: Customer Impact
RiskDescription: The security breach occurred due to unauthorized access by hackers, leading to pote
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 6.48
RiskMultiplierX: 0.3
RiskMultiplierY: 0.3
RiskPriority: High
RiskMitigation: Implement multi-factor authentication for all system access to prevent unauthorized log
CreatedAt: 2025-10-22 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1373:
RiskId: 1305
ComplianceId: 1959
RiskTitle: Basel III Capital Conservation Buffer (CCB) Compliance Compliance Type
Criticality: Low
PossibleDamage: Misreporting of CET1 due to data reconciliation issues between finance and regulato
Category: External Risk
RiskType: Current
BusinessImpact: Customer Impact
RiskDescription: This compliance item ensures adherence to the Basel III Capital Conservation Buffer
RiskLikelihood: 5
RiskImpact: 5
RiskExposureRating: 25
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: None
CreatedAt: 2025-10-14 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1374:
RiskId: 1306
ComplianceId: 1962
RiskTitle: Compliance 1
Criticality: Medium
PossibleDamage: Risk kkkkkkkkkkkkk1
Category: External Risk
RiskType: Residual
BusinessImpact: Brand Damage
RiskDescription: Descriptionnnnnnnnnn 1
RiskLikelihood: 5
RiskImpact: 5
RiskExposureRating: 25
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: None
CreatedAt: 2025-10-14 00:00:00
CreatedBy: audit.dept.rajiv.khanna
CreatedByName: Rajiv Khanna
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1375:
RiskId: 1307
ComplianceId: 1
RiskTitle: Emerging risk
Criticality: High
PossibleDamage: Potential data breaches leading to financial losses and reputational damage

Category: Process Risk
RiskType: Current
BusinessImpact: Operational Disruption, Customer Impact
RiskDescription: Description1
RiskLikelihood: 1
RiskImpact: 1
RiskExposureRating: 0.02
RiskMultiplierX: 0.1
RiskMultiplierY: 0.2
RiskPriority: High
RiskMitigation: Action1
CreatedAt: 2025-10-14 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1376:
RiskId: 1301
ComplianceId: 1955
RiskTitle: Annual Review of PCI-Approved ASV Vendors
Criticality: High
PossibleDamage: Selection of an ASV with inadequate security measures leading to a data breach
Category: Operational
RiskType: Current
BusinessImpact: All departments involved in payment processin
RiskDescription: Organizations must annually review the list of PCI-approved vendors on the PCI Secu
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: None
CreatedAt: 2025-10-12 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1377:
RiskId: 1302
ComplianceId: 1956
RiskTitle: Qualifications Evaluation of ASVs
Criticality: Medium
PossibleDamage: Inadequate security assessment leading to undetected vulnerabilities
Category: IT
RiskType: Current
BusinessImpact: All departments involved in payment processin
RiskDescription: The selection process should include evaluating the ASV's qualifications, experience,
RiskLikelihood: 6
RiskImpact: 6
RiskExposureRating: 36
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: None
CreatedAt: 2025-10-12 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1378:
RiskId: 1303
ComplianceId: 1957
RiskTitle: Formalize ASV Engagement through Contract
Criticality: High
PossibleDamage: ASV engagement delays, incomplete deliverables, security vulnerabilities
Category: Operational
RiskType: Residual
BusinessImpact: Compliance Officer, IT Security Team
RiskDescription: Once an ASV is selected, the organization must formalize the engagement through a

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: None
CreatedAt: 2025-10-12 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1379:
RiskId: 1304
ComplianceId: 1958
RiskTitle: Timely Vulnerability Scan Reporting
Criticality: Medium
PossibleDamage: Delayed identification of vulnerabilities, increased risk of data breaches
Category: Operational
RiskType: Residual
BusinessImpact: ASV Provider, IT Security Team
RiskDescription: ASV must provide detailed vulnerability scan reports within 5 business days of scan c
RiskLikelihood: 6
RiskImpact: 6
RiskExposureRating: 36
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: None
CreatedAt: 2025-10-12 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1380:
RiskId: 1152

ComplianceId: 1802
RiskTitle: Non-Compliance with ISMS Policy
Criticality: High
PossibleDamage: Confusion and lack of direction in information security management
Category: Operational
RiskType: Residual
BusinessImpact: Disruption to information security management processes
RiskDescription: Failure to maintain the approved ISMS policy may result in ineffective information sec
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the ISMS policy", "2": "Provide training to ensure un
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1381:
RiskId: 1153
ComplianceId: 1803
RiskTitle: Outdated ISMS Policy
Criticality: High
PossibleDamage: Increased security vulnerabilities
Category: Operational
RiskType: Residual
BusinessImpact: Potential data breaches and regulatory fines
RiskDescription: Failure to update the ISMS policy annually may result in outdated security measures a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular policy reviews", "2": "Change management process for updates", "3": "Er

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1382:

RiskId: 1154

ComplianceId: 1804

RiskTitle: Non-Compliance due to Unmanaged Policy Exceptions

Criticality: High

PossibleDamage: Financial penalties, legal actions, reputational damage.

Category: Compliance

RiskType: Residual

BusinessImpact: Potential loss of business opportunities and damage to reputation.

RiskDescription: Failure to manage policy exceptions could result in violations of regulations and interr

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular review and update of policy exceptions", "2": "Training for employees on

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Compliance Division

Item 1383:

RiskId: 1155

ComplianceId: 1805

RiskTitle: Unauthorized Access Risk

Criticality: Medium

PossibleDamage: Data breaches, loss of sensitive information

Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Users accessing systems without acknowledging policies may lead to unauthorized a
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular policy training sessions", "2": "Strong access controls", "3": "Continuous m
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1384:
RiskId: 1156
ComplianceId: 1806
RiskTitle: Confusion in ISMS roles
Criticality: High
PossibleDamage: Increased security risks and non-compliance with regulations
Category: Operational
RiskType: Residual
BusinessImpact: Potential security incidents affecting confidentiality, integrity, and availability of inform
RiskDescription: Lack of clear roles and responsibilities may lead to mismanagement of security contro
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on ISMS roles and responsibilities", "2"
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1385:
RiskId: 1157
ComplianceId: 1807
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Financial loss, reputational damage, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Unauthorized access to sensitive data or systems due to lack of segregation of duties
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement RBAC controls", "2": "Regularly review access permissions", "3": "Prov
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1386:
RiskId: 1158
ComplianceId: 1808
RiskTitle: Failure to Designate Points of Contact
Criticality: High
PossibleDamage: Delayed or inadequate responses to legal and regulatory inquiries, potential fines or
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to designate points of contact for legal and regulatory liaison may result in inef

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and updates for designated points of contact on legal and regula
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1387:
RiskId: 1159
ComplianceId: 1809
RiskTitle: Lack of Community Participation
Criticality: Medium
PossibleDamage: Delayed threat detection and response
Category: Operational
RiskType: Residual
BusinessImpact: Potential security incidents affecting business operations
RiskDescription: Failure to actively participate in security communities may result in missing critical thr
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear participation guidelines", "2": "Regularly review and assess the be
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1388:
RiskId: 1160

ComplianceId: 1810
RiskTitle: Data Breach Due to Inadequate Security Measures
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal penalties
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines, operational disruptions
RiskDescription: Failure to embed security requirements in project lifecycles may lead to vulnerabilities
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security assessments and audits", "2": "Implementation of encryption and
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1389:
RiskId: 1161
ComplianceId: 1811
RiskTitle: Data Breach due to Unmanaged Mobile Devices
Criticality: High
PossibleDamage: Financial loss, reputational damage, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Unauthorized access to sensitive data on unmanaged mobile devices could lead to a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement MDM solution", "2": "Regular security training for employees", "3": "En
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1390:
RiskId: 1162
ComplianceId: 1812
RiskTitle: Data Breach due to Lack of Encryption
Criticality: Medium
PossibleDamage: Loss of sensitive data, regulatory fines, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Disruption of IT operations, loss of customer trust
RiskDescription: Sensitive data stored on unencrypted mobile devices could be accessed by unauthori
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enforce encryption on all devices", "2": "Regular encryption key management", "3
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1391:
RiskId: 1163
ComplianceId: 1813
RiskTitle: Data Exposure due to Lack of Screen Lock
Criticality: Low
PossibleDamage: Loss of sensitive data, reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions, loss of customer trust
RiskDescription: Devices without screen lock enabled could be accessed by unauthorized individuals,
RiskLikelihood: 5
RiskImpact: 4
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Enforce screen lock policies through MDM", "2": "Regular employee training on sc
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1392:
RiskId: 1164
ComplianceId: 1814
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation
RiskDescription: Unauthorized access to company systems and data due to lack of VPN usage
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enforce VPN usage through policy and monitoring", "2": "Regularly update VPN s
CreatedAt: 2025-10-11 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1393:
RiskId: 1165
ComplianceId: 1815
RiskTitle: MFA Non-Compliance Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation
RiskDescription: Unauthorized access to company systems and data due to lack of MFA usage
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 60
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enforce MFA usage through policy and monitoring", "2": "Regularly update MFA p
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1394:
RiskId: 1166
ComplianceId: 1816
RiskTitle: Home Office Security Risk
Criticality: Medium
PossibleDamage: Physical security breaches, unauthorized access
Category: Operational
RiskType: Current
BusinessImpact: Disruption of work, potential data loss
RiskDescription: Lack of secure home office standards leading to physical breaches or unauthorized a

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide guidelines for secure home office setup", "2": "Regularly audit home office
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1395:
RiskId: 1167
ComplianceId: 1817
RiskTitle: Risk of Hiring Unqualified or Dishonest Employees
Criticality: High
PossibleDamage: Legal issues, financial losses, damage to company reputation
Category: Operational
RiskType: Inherent
BusinessImpact: Potential legal liabilities, decreased productivity, negative impact on company culture
RiskDescription: Failure to conduct thorough background checks may result in hiring individuals who d
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement stringent background verification processes", "2": "Train HR staff on id
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1396:
RiskId: 1168

ComplianceId: 1818
RiskTitle: Confidentiality Breach Risk
Criticality: High
PossibleDamage: Loss of sensitive information, legal liabilities, reputational damage.
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, legal consequences.
RiskDescription: Failure to maintain confidentiality could result in unauthorized access to sensitive data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update confidentiality policies", "2": "Implement encryption a
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1397:
RiskId: 1169
ComplianceId: 1819
RiskTitle: Acceptable Use Policy Violation Risk
Criticality: Medium
PossibleDamage: Data breaches, system misuse, legal repercussions.
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, legal consequences.
RiskDescription: Failure to comply with acceptable use policies could result in unauthorized access to s
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly communicate and reinforce acceptable use policies", "2": "Implement a

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 1398:

RiskId: 1170

ComplianceId: 1820

RiskTitle: Employee Vulnerability to Social Engineering Attacks

Criticality: High

PossibleDamage: Loss of sensitive data, financial loss, reputational damage

Category: Operational

RiskType: Residual

BusinessImpact: Disruption of operations, financial loss, damage to reputation

RiskDescription: Employees unknowingly disclosing sensitive information to malicious actors through s

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Provide regular training on social engineering tactics and how to identify them", "2

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 1399:

RiskId: 1171

ComplianceId: 1821

RiskTitle: Security Breach Risk

Criticality: High

PossibleDamage: Financial loss, reputational damage, legal consequences

Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: The risk of security breaches leading to unauthorized access to sensitive information
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly update security patches",
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1400:
RiskId: 1172
ComplianceId: 1822
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Loss of sensitive data, financial loss.
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Former employees retaining access to systems and data, leading to potential data bre
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review access rights", "2": "Implement two-factor authentication", "3": "E
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1401:
RiskId: 1173
ComplianceId: 1823
RiskTitle: Inaccurate Asset Tracking
Criticality: High
PossibleDamage: Financial losses, security breaches
Category: Operational
RiskType: Current
BusinessImpact: Loss of assets, compromised security
RiskDescription: Failure to maintain an accurate inventory of assets can lead to financial losses and se
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of the CMDB/asset register", "2": "Training for employees on asset
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1402:
RiskId: 1174
ComplianceId: 1824
RiskTitle: Asset Ownership Documentation Risk
Criticality: High
PossibleDamage: Loss or misuse of assets, legal consequences.
Category: Operational
RiskType: Current
BusinessImpact: Loss of assets, legal liabilities.
RiskDescription: Failure to document asset ownership can lead to confusion, misuse, or loss of assets

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to verify ownership documentation", "2": "Training on asset owners
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1403:
RiskId: 1175
ComplianceId: 1825
RiskTitle: Non-Compliance with Asset Return Policy
Criticality: High
PossibleDamage: Loss of sensitive data, unauthorized access, financial loss
Category: Operational
RiskType: Current
BusinessImpact: Data breaches, financial losses, reputational damage
RiskDescription: Failure to verify return of assets can lead to unauthorized access to sensitive informat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict exit procedures for asset return", "2": "Regularly update asset inv
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1404:
RiskId: 1176

ComplianceId: 1826
RiskTitle: Malware Infection Due to Unauthorized Software
Criticality: High
PossibleDamage: Data loss, system compromise, financial loss
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, loss of sensitive data
RiskDescription: Unauthorized software may contain malware that can infect corporate devices and co
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular software audits", "2": "Endpoint protection software", "3": "User access co
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1405:
RiskId: 1177
ComplianceId: 1827
RiskTitle: Data Breach Due to Personal Data Storage
Criticality: Medium
PossibleDamage: Loss of customer trust, regulatory fines, legal action
Category: Compliance
RiskType: Residual
BusinessImpact: Reputational damage, financial penalties
RiskDescription: Storing personal data on corporate devices increases the risk of data breaches and n
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Data encryption on devices", "2": "Employee awareness programs", "3": "Regular
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1406:
RiskId: 1178
ComplianceId: 1828
RiskTitle: Data Breach Due to Unauthorized Email Access
Criticality: High
PossibleDamage: Loss of sensitive data, legal penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Unauthorized access to company email accounts could lead to leakage of sensitive in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls to email accounts", "2": "Regularly update securi
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1407:
RiskId: 1179
ComplianceId: 1829
RiskTitle: Data Breach due to Unenrolled Personal Devices
Criticality: High
PossibleDamage: Loss of sensitive company data, reputational damage, financial losses

Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of business operations, legal consequences, loss of customer trust
RiskDescription: If personal devices are not enrolled, there is a high risk of data breaches and unautho
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enforce strict enrollment policies", "2": "Regularly monitor enrolled devices for cor
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1408:
RiskId: 1180
ComplianceId: 1830
RiskTitle: Data Breach due to Unencrypted Personal Devices
Criticality: High
PossibleDamage: Loss of sensitive company data, reputational damage, legal consequences
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of business operations, financial losses, regulatory fines
RiskDescription: If personal devices are not encrypted, there is a high risk of data breaches and non-c
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enforce encryption policies through device management system", "2": "Regularly
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1409:
RiskId: 1181
ComplianceId: 1831
RiskTitle: Data Breach due to Lack of Remote Wipe-on-Loss Capability
Criticality: High
PossibleDamage: Loss of sensitive company data, reputational damage, financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of business operations, legal consequences, loss of customer trust
RiskDescription: If personal devices do not have remote wipe capabilities, there is a high risk of unauth
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly test remote wipe capabilities", "2": "Provide training on remote wipe pro
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1410:
RiskId: 1182
ComplianceId: 1832
RiskTitle: Data Breach due to Misclassification
Criticality: High
PossibleDamage: Data exposure, reputational damage, regulatory fines
Category: Compliance
RiskType: Inherent
BusinessImpact: Significant financial and reputational damage
RiskDescription: Misclassification of sensitive data could lead to unauthorized access and data breach

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular classification reviews", "2": "Implement data loss prevention tools", "3": "E
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1411:
RiskId: 1183
ComplianceId: 1833
RiskTitle: Data Breach due to Mislabeling of Sensitive Information
Criticality: High
PossibleDamage: Financial loss, reputational damage, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Mislabeling of sensitive data could lead to unauthorized access, data breaches, and r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated labeling tools", "2": "Regularly review and update labeling p
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1412:
RiskId: 1184

ComplianceId: 1834
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data breaches leading to financial losses and reputational damage
Category: IT
RiskType: Current
BusinessImpact: Loss of customer trust, regulatory fines, legal actions
RiskDescription: Unauthorized access to confidential data due to lack of encryption measures
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption protocols", "2": "Regularly monitor access logs", "3": "Cond
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1413:
RiskId: 1185
ComplianceId: 1835
RiskTitle: Information Mishandling Risk
Criticality: Medium
PossibleDamage: Data leaks and compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, reputational damage
RiskDescription: Improper handling of sensitive information leading to leaks or compliance issues
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement classification controls", "2": "Provide regular training on handling proce
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1414:
RiskId: 1186
ComplianceId: 1836
RiskTitle: Data Breach Due to Improper Destruction
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties, legal consequences
RiskDescription: Failure to use approved destruction methods may result in unauthorized access to se
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on approved destruction methods", "2": "Periodic audits to ensure
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1415:
RiskId: 1187
ComplianceId: 1837
RiskTitle: Inability to Prove Compliance Due to Lack of Certificates
Criticality: Medium
PossibleDamage: Legal issues, penalties

Category: Compliance
RiskType: Current
BusinessImpact: Penalties, reputational damage
RiskDescription: Failure to maintain destruction certificates may result in the inability to prove complian
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a robust documentation process", "2": "Regularly review and update d
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1416:
RiskId: 1188
ComplianceId: 1838
RiskTitle: Unauthorized Data Access and Data Breach
Criticality: High
PossibleDamage: Data loss, reputational damage, financial loss
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data and customer trust
RiskDescription: Unauthorized access to sensitive data due to uncontrolled removable media usage.
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement data encryption on removable media", "2": "Regularly educate employ
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1417:
RiskId: 1189
ComplianceId: 1839
RiskTitle: Data Breach due to Improper Media Disposal
Criticality: High
PossibleDamage: Data breach resulting in financial losses, reputational damage, and legal consequen
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, regulatory fines, legal actions
RiskDescription: Improper media disposal could lead to unauthorized access to sensitive information, r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement secure disposal procedures", "2": "Encrypt sensitive data before dispo
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1418:
RiskId: 1190
ComplianceId: 1840
RiskTitle: Unauthorized Access to Sensitive Information during Physical Media Transfer
Criticality: High
PossibleDamage: Data breaches, loss of confidential data, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines, legal implications
RiskDescription: Unauthorized access to sensitive information during physical media transfer can lead

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls for physical media handling", "2": "Regularly aud
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1419:
RiskId: 1191
ComplianceId: 1841
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, financial losses.
Category: Operational
RiskType: Current
BusinessImpact: Disruption of business operations, reputational damage.
RiskDescription: Unauthorized access to critical systems and sensitive data can lead to data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access control", "2": "Regularly review and update access
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1420:
RiskId: 1192

ComplianceId: 1842
RiskTitle: Unauthorized Network Access
Criticality: High
PossibleDamage: Data breaches, network downtime, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, financial losses, regulatory fines
RiskDescription: Unauthorized users gaining access to sensitive data and network resources
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access control policies", "2": "Regularly audit network access log
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1421:
RiskId: 1193
ComplianceId: 1843
RiskTitle: Delayed User Provisioning
Criticality: High
PossibleDamage: Unauthorized access, service disruptions
Category: Operational
RiskType: Residual
BusinessImpact: Potential security breaches and data leaks
RiskDescription: Failure to provision user accounts within SLAs could lead to unauthorized access to s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Automate provisioning processes to reduce delays", "2": "Implement multi-factor a
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1422:
RiskId: 1194
ComplianceId: 1844
RiskTitle: Delayed User De-provisioning
Criticality: High
PossibleDamage: Unauthorized access, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Potential data breaches and loss of sensitive information
RiskDescription: Failure to de-provision user accounts promptly could result in unauthorized access to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate de-provisioning processes to reduce delays", "2": "Implement strict acc
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1423:
RiskId: 1195
ComplianceId: 1845
RiskTitle: Data Breach Due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage, legal consequences.

Category: Operational
RiskType: Current
BusinessImpact: Significant financial and reputational damage.
RiskDescription: Unauthorized access to sensitive data could lead to data breaches and compliance vi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly review and update access
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1424:
RiskId: 1196
ComplianceId: 1846
RiskTitle: Unauthorized Access to Critical Systems
Criticality: High
PossibleDamage: Data breaches, financial loss, reputational damage
Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, loss of sensitive data
RiskDescription: Unauthorized access to privileged accounts could lead to data breaches and compron
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and monitoring for privileged accounts", "2": "Re
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1425:
RiskId: 1197
ComplianceId: 1847
RiskTitle: Undetected Malicious Activities
Criticality: Medium
PossibleDamage: Data breaches, financial loss, reputational damage
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive data, operational disruptions
RiskDescription: Failure to record and monitor privileged sessions could lead to undetected malicious a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement real-time session monitoring and alerts", "2": "Regularly review sessio
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1426:
RiskId: 1198
ComplianceId: 1848
RiskTitle: Compromised Credentials
Criticality: High
PossibleDamage: Unauthorized access to sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Data breaches and loss of trust
RiskDescription: Outdated or compromised credentials could lead to unauthorized access to sensitive

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enforce strong password policies", "2": "Implement multi-factor authentication", "3
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1427:
RiskId: 1199
ComplianceId: 1849
RiskTitle: Unauthorized Vault Access
Criticality: High
PossibleDamage: Data breaches and loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Data breaches and loss of trust
RiskDescription: Unauthorized access to the secure vault could lead to exposure of sensitive informati
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls", "2": "Encrypt all stored secrets", "3": "Regular
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1428:
RiskId: 1200

ComplianceId: 1850
RiskTitle: Data Breach due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Significant financial and reputational damage
RiskDescription: Unauthorized access to sensitive data could lead to data breaches and financial losse
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly monitor access logs for unu
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1429:
RiskId: 1201
ComplianceId: 1851
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to critical systems and data
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, reputational damage
RiskDescription: Unauthorized individuals gaining access to critical systems and data, leading to poten
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Regularly educate users on password
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1430:
RiskId: 1202
ComplianceId: 1852
RiskTitle: Unauthorized Access Risk to Critical Systems
Criticality: Critical
PossibleDamage: Unauthorized access to critical systems and data
Category: Operational
RiskType: Residual
BusinessImpact: Loss of critical data, operational disruptions
RiskDescription: Unauthorized individuals gaining access to critical systems and data, leading to poten
RiskLikelihood: 9
RiskImpact: 10
RiskExposureRating: 90
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication solutions", "2": "Regularly review and updat
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1431:
RiskId: 1203
ComplianceId: 1853
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to confidential data, data breaches

Category: IT
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Unauthorized individuals gaining access to sensitive information stored on workstatio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Encrypt sensitive data on workstation
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1432:
RiskId: 1204
ComplianceId: 1854
RiskTitle: Delayed Incident Response Risk
Criticality: Medium
PossibleDamage: Delayed response to security incidents, increased risk of data breaches
Category: IT
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to promptly report and address suspicious activity on workstations may lead to
RiskLikelihood: 6
RiskImpact: 6
RiskExposureRating: 36
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish incident response team", "2": "Conduct regular security awareness train
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1433:
RiskId: 1205
ComplianceId: 1855
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Loss of confidentiality, data breaches
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation
RiskDescription: Unauthorized individuals gaining access to sensitive information can lead to data brea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews to ensure permissions are up to date", "2": "Implement m
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1434:
RiskId: 1206
ComplianceId: 1856
RiskTitle: Data Breach Due to Lack of MFA
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage.
Category: Operational
RiskType: Residual
BusinessImpact: Significant financial loss, damage to reputation, legal consequences.
RiskDescription: Unauthorized users gaining access to sensitive information due to lack of MFA, leadi

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement MFA solutions immediately", "2": "Regularly monitor MFA usage and e
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1435:
RiskId: 1207
ComplianceId: 1857
RiskTitle: Data Breach Due to Lack of Session Timeout
Criticality: Medium
PossibleDamage: Unauthorized access to active sessions, data breaches, information leakage.
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, reputational damage, legal consequences.
RiskDescription: Unauthorized users gaining access to active sessions left unattended, leading to data
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement session timeout policies immediately", "2": "Educate users on session
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1436:
RiskId: 1208

ComplianceId: 1858
RiskTitle: Brute Force Attack Due to Lack of Account Lockout
Criticality: High
PossibleDamage: System downtime, unauthorized access, data breaches.
Category: Operational
RiskType: Residual
BusinessImpact: Significant system downtime, financial loss, reputational damage.
RiskDescription: Malicious actors attempting to gain unauthorized access through brute force attacks c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement account lockout policies immediately", "2": "Monitor failed login attemp
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1437:
RiskId: 1209
ComplianceId: 1859
RiskTitle: Risk of Weak Passwords
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, financial losses.
Category: Operational
RiskType: Residual
BusinessImpact: Potential unauthorized access to sensitive data and financial losses.
RiskDescription: Weak passwords can be easily compromised, leading to unauthorized access and po
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Enforce password complexity requirements", "2": "Implement multi-factor authenti

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1438:

RiskId: 1210

ComplianceId: 1860

RiskTitle: Risk of Infrequent Password Resets

Criticality: Medium

PossibleDamage: Unauthorized access to sensitive information, data breaches, financial losses.

Category: Operational

RiskType: Residual

BusinessImpact: Potential unauthorized access to sensitive data and financial losses.

RiskDescription: Infrequent password resets increase the likelihood of compromised passwords and u

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement password expiration policy", "2": "Provide user notifications for passwo

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1439:

RiskId: 1211

ComplianceId: 1861

RiskTitle: Unauthorized Access to Sensitive Information

Criticality: High

PossibleDamage: Data breaches, loss of sensitive information, reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, legal consequences, damage to reputation
RiskDescription: Unauthorized access to sensitive information can lead to data breaches, loss of intelle
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access controls", "2": "Implement strong authenticat
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1440:
RiskId: 1212
ComplianceId: 1862
RiskTitle: Unauthorized Source Code Access
Criticality: High
PossibleDamage: Security breaches, intellectual property theft, compromised software integrity
Category: Operational
RiskType: Current
BusinessImpact: Development, IT
RiskDescription: Unauthorized access to source code repositories can lead to unauthorized modificatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access control with least privilege principle", "2": "Enforce r
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1441:
RiskId: 1213
ComplianceId: 1863
RiskTitle: Use of Weak Cryptographic Algorithms
Criticality: High
PossibleDamage: Data breaches, compromised security, regulatory fines
Category: IT
RiskType: Residual
BusinessImpact: Compromised security and potential data breaches affecting all business units.
RiskDescription: The use of weak or deprecated cryptographic algorithms can lead to unauthorized ac
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update cryptographic algorithms", "2": "Implement multi-factor authentic
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1442:
RiskId: 1214
ComplianceId: 1864
RiskTitle: Data Breach due to Key Mismanagement
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, legal consequences, loss of customer trust
RiskDescription: Failure to properly manage encryption keys could lead to unauthorized access to sen

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement HSM/KMS for key management", "2": "Enforce key rotation policies", "
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1443:
RiskId: 1215
ComplianceId: 1865
RiskTitle: Unauthorized Access to Secure Areas
Criticality: High
PossibleDamage: Unauthorized access to sensitive information or assets
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, theft of assets, or compromise of security measures
RiskDescription: Unauthorized individuals gaining access to secure areas can lead to data breaches, t
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security audits and inspections", "2": "Employee training on access contr
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1444:
RiskId: 1216

ComplianceId: 1866
RiskTitle: Unauthorized Access Control Breach
Criticality: Medium
PossibleDamage: Unauthorized access leading to security breaches
Category: Operational
RiskType: Current
BusinessImpact: Compromise of security measures and potential data breaches
RiskDescription: Failure to restrict access to secure areas can result in unauthorized individuals gainin
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular access control audits", "2": "Implementing biometric authentication for hig
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1445:
RiskId: 1217
ComplianceId: 1867
RiskTitle: Unauthorized Access to Secure Areas
Criticality: High
PossibleDamage: Theft of sensitive data, physical assets, or compromise of security measures.
Category: Operational
RiskType: Residual
BusinessImpact: Loss of trust, financial implications, legal consequences.
RiskDescription: Unauthorized individuals gaining access to secure areas due to lack of access logs ar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement biometric access control", "2": "Regularly review access logs for anom
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1446:
RiskId: 1218
ComplianceId: 1868
RiskTitle: Inadequate Video Surveillance Coverage
Criticality: Medium
PossibleDamage: Lack of visual evidence in case of security incidents or breaches.
Category: Operational
RiskType: Residual
BusinessImpact: Inability to investigate security incidents effectively, potential legal implications.
RiskDescription: Insufficient video surveillance coverage in secure areas leading to gaps in monitoring
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular maintenance and testing of surveillance cameras", "2": "Encrypt video fo
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1447:
RiskId: 1219
ComplianceId: 1869
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, theft of sensitive information.

Category: Operational

RiskType: Residual

BusinessImpact: Loss of customer trust, financial penalties.

RiskDescription: Unauthorized individuals gaining access to sensitive information stored in cabinets.

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement access control systems", "2": "Encrypt sensitive information", "3": "Reg

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 1448:

RiskId: 1220

ComplianceId: 1870

RiskTitle: Unauthorized Access by Visitors

Criticality: Medium

PossibleDamage: Theft of information, compromise of security measures.

Category: Operational

RiskType: Residual

BusinessImpact: Loss of confidential information, compromised security.

RiskDescription: Visitors gaining unauthorized access to restricted areas or sensitive information.

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement visitor registration system", "2": "Escort visitors at all times", "3": "Regu

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1449:
RiskId: 1221
ComplianceId: 1871
RiskTitle: Failure to Detect Environmental Threats
Criticality: High
PossibleDamage: Equipment damage, downtime, and potential safety hazards
Category: Environmental
RiskType: Inherent
BusinessImpact: Disruption of operations and potential safety risks to personnel
RiskDescription: Undetected environmental threats can lead to equipment failure, downtime, and poter
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular maintenance and calibration of sensors", "2": "Automated alerts for abnor
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1450:
RiskId: 1222
ComplianceId: 1872
RiskTitle: Lack of Redundancies for Power and HVAC Systems
Criticality: High
PossibleDamage: Disruptions in operations, loss of productivity, and potential equipment damage
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of productivity, potential equipment damage, and financial losses
RiskDescription: Failure to have redundancies for power and HVAC systems can lead to disruptions in

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing of backup power sources", "2": "Scheduled maintenance of HVAC
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1451:
RiskId: 1223
ComplianceId: 1873
RiskTitle: Unauthorized Access to Secure Areas
Criticality: High
PossibleDamage: Data breaches, theft of sensitive information, compromise of security measures
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, damage to reputation
RiskDescription: Unauthorized individuals gaining access to secure areas can lead to data breaches a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access control measures", "2": "Regular security training for emp
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1452:
RiskId: 1224

ComplianceId: 1874
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: Medium
PossibleDamage: Data breaches, compromise of security measures, theft of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, damage to reputation, legal consequences
RiskDescription: Leaving sensitive information unattended on desks or screens can lead to unauthorize
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement clear desk/screen policy and regular checks", "2": "Encryption of sensi
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1453:
RiskId: 1225
ComplianceId: 1875
RiskTitle: Unauthorized Access to Loading Bays
Criticality: High
PossibleDamage: Theft, sabotage, security breaches
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, damage to reputation
RiskDescription: Unauthorized access to loading bays can result in theft of goods, tampering with prod
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement access control systems at loading bay entrances", "2": "Regularly mon
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1454:
RiskId: 1226
ComplianceId: 1876
RiskTitle: Unauthorized Access through Delivery Routes
Criticality: Medium
PossibleDamage: Compromised security measures, breach of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Security vulnerabilities, operational disruptions
RiskDescription: Unauthorized access through delivery routes can compromise security measures and
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement physical barriers between delivery routes and secure areas", "2": "Use
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1455:
RiskId: 1227
ComplianceId: 1877
RiskTitle: Data Breach due to Unsecured Desk
Criticality: High
PossibleDamage: Loss of confidential data, reputational damage, financial penalties

Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, damage to reputation
RiskDescription: Unauthorized access to sensitive information left on unsecured desks could lead to da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement clear desk policy and training for all employees", "2": "Regularly monito
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1456:
RiskId: 1228
ComplianceId: 1878
RiskTitle: Unauthorized Access to Sensitive Data
Criticality: High
PossibleDamage: Data breaches, financial loss, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Unauthorized individuals gaining access to sensitive data due to unlocked screens
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security awareness training for employees", "2": "Implement data loss pre
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1457:
RiskId: 1229
ComplianceId: 1879
RiskTitle: Unauthorized Viewing of Sensitive Apps
Criticality: Medium
PossibleDamage: Data breaches, financial loss
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of competitive advantage, regulatory fines
RiskDescription: Unauthorized individuals viewing sensitive app content due to lack of masking
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular security assessments of app hiding mechanisms", "2": "Implement acces
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1458:
RiskId: 1230
ComplianceId: 1880
RiskTitle: Outdated SOPs Risk
Criticality: High
PossibleDamage: Errors, inefficiencies, non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions, compliance issues
RiskDescription: Outdated SOPs may result in employees following incorrect procedures, leading to er

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on SOP updates", "2": "Automated version control system", "3": "
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1459:
RiskId: 1231
ComplianceId: 1881
RiskTitle: Unapproved Operational Changes
Criticality: High
PossibleDamage: System downtime, data loss, security breaches
Category: Operational
RiskType: Residual
BusinessImpact: Disruption to operations, financial losses
RiskDescription: Unauthorized operational changes can lead to system instability, data corruption, or s
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Strict change approval process", "2": "Regular monitoring for unauthorized chang
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1460:
RiskId: 1232

ComplianceId: 1882
RiskTitle: Capacity Threshold Breach
Criticality: High
PossibleDamage: System downtime, performance degradation, revenue loss
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Failure to set and monitor capacity thresholds may result in system failures and perfo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools for real-time capacity tracking", "2": "Estab
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1461:
RiskId: 1233
ComplianceId: 1883
RiskTitle: Inadequate Capacity Planning
Criticality: Medium
PossibleDamage: Resource shortages, service disruptions, increased costs
Category: Operational
RiskType: Residual
BusinessImpact: Operational inefficiencies, financial losses, customer dissatisfaction
RiskDescription: Lack of effective capacity planning may lead to under or overprovisioning of resources
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement capacity management tools for accurate forecasting", "2": "Regularly r

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1462:

RiskId: 1234

ComplianceId: 1884

RiskTitle: Unauthorized Access Risk

Criticality: High

PossibleDamage: Data breaches, unauthorized access to sensitive information

Category: IT

RiskType: Residual

BusinessImpact: Potential compromise of sensitive data, disruption of services

RiskDescription: Risk of unauthorized access to production data due to lack of network segregation be

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strict firewall rules to restrict access between environments", "2": "Use

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1463:

RiskId: 1235

ComplianceId: 1885

RiskTitle: Access Control Risk

Criticality: Medium

PossibleDamage: Unauthorized access, data manipulation

Category: IT
RiskType: Residual
BusinessImpact: Potential compromise of data integrity, security breaches
RiskDescription: Risk of unauthorized access and data manipulation due to inadequate access control
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement role-based access control to restrict access based on job roles", "2": "U
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1464:
RiskId: 1236
ComplianceId: 1886
RiskTitle: Malware Infections and Data Breaches
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, system downtime, financial losses
RiskDescription: Failure to deploy EDR/AV could result in malware infections, data breaches, and finar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular updates and patches for EDR/AV software", "2": "Continuous monitoring
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1465:
RiskId: 1237
ComplianceId: 1887
RiskTitle: Data Loss Risk
Criticality: High
PossibleDamage: Loss of critical information, system downtime
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Failure to backup data could result in permanent loss of critical information and syste
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly test backup integrity", "2": "Implement redundancy in backup systems",
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1466:
RiskId: 1238
ComplianceId: 1888
RiskTitle: Data Retention Risk
Criticality: Medium
PossibleDamage: Legal penalties, inability to recover critical information
Category: Operational
RiskType: Inherent
BusinessImpact: Legal consequences, operational disruptions
RiskDescription: Failure to adhere to backup retention policies could result in legal non-compliance an

RiskLikelihood: 7
RiskImpact: 7
RiskExposureRating: 52.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly audit retention practices", "2": "Implement legal review of retention polic
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1467:
RiskId: 1239
ComplianceId: 1889
RiskTitle: Backup Testing Risk
Criticality: High
PossibleDamage: Inability to recover critical data, data corruption
Category: IT
RiskType: Inherent
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Failure to conduct regular restore tests could result in the inability to recover critical da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate restore testing processes", "2": "Implement continuous monitoring of ba
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1468:
RiskId: 1240

ComplianceId: 1890
RiskTitle: Inadequate Event Logging
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats, delayed incident response, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Disruption of IT operations, data breaches, non-compliance penalties
RiskDescription: Failure to centralize logs in SIEM with time sync may lead to undetected security incid
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and review of logs for suspicious activities", "2": "Implementat
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1469:
RiskId: 1241
ComplianceId: 1891
RiskTitle: Unauthorized access to log data
Criticality: High
PossibleDamage: Data breaches, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, financial penalties
RiskDescription: Unauthorized access to log data can lead to security breaches and non-compliance w
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strict access controls to limit who can view log data", "2": "Regularly au

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1470:

RiskId: 1242

ComplianceId: 1892

RiskTitle: Risk of Undetected Unauthorized Activities

Criticality: High

PossibleDamage: System compromise, data breaches

Category: Operational

RiskType: Current

BusinessImpact: Disruption of IT operations, loss of sensitive data

RiskDescription: Failure to record admin sessions and commands can result in undetected malicious a

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement multi-factor authentication for admin access", "2": "Regularly review ac

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 1471:

RiskId: 1243

ComplianceId: 1893

RiskTitle: Data Inconsistencies and Security Vulnerabilities

Criticality: High

PossibleDamage: Unauthorized access, data corruption, and security breaches

Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, reputation damage, financial losses
RiskDescription: Failure to synchronize system clocks may lead to inaccurate timestamps, causing dat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated clock synchronization processes", "2": "Regularly review ar
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1472:
RiskId: 1244
ComplianceId: 1894
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information leading to data breaches and loss of c
Category: Operational
RiskType: Residual
BusinessImpact: Loss of confidential data, reputational damage, financial losses
RiskDescription: Unauthorized access to sensitive information can lead to data breaches, loss of confi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for enhanced security", "2": "Enforce regula
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1473:
RiskId: 1245
ComplianceId: 1895
RiskTitle: Role-Based Access Control Risk
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information, data breaches, and potential misuse o
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, loss of confidentiality, reputational damage
RiskDescription: Improper role assignments or lack of role-based access control can lead to unauthoriz
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update role assignments based on job responsibilities", "2":
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1474:
RiskId: 1246
ComplianceId: 1896
RiskTitle: Failure to Establish Incident Response Team
Criticality: High
PossibleDamage: Data breaches, system compromises, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Significant disruption to business operations, financial losses, regulatory fines
RiskDescription: Inadequate incident response team may lead to delayed or ineffective handling of sec

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and updates for team members", "2": "Periodic drills to test team
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1475:
RiskId: 1247
ComplianceId: 1897
RiskTitle: Lack of Incident Response Plan
Criticality: Medium
PossibleDamage: Confusion, delays, inadequate response to security incidents
Category: Operational
RiskType: Current
BusinessImpact: Disruption to business operations, financial losses, regulatory penalties
RiskDescription: Absence of a structured incident response plan may lead to confusion, delays, and in
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update of the plan", "2": "Training and awareness sessions or
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1476:
RiskId: 1248

ComplianceId: 1898
RiskTitle: Confusion in Information Security Roles
Criticality: Medium
PossibleDamage: Confusion and lack of accountability in information security management
Category: Operational
RiskType: Current
BusinessImpact: Potential security breaches and data leaks
RiskDescription: Failure to clearly define and communicate information security roles can lead to mism
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training and communication on roles and responsibilities", "2": "Establish
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1477:
RiskId: 1249
ComplianceId: 1899
RiskTitle: Outdated Information Security Roles
Criticality: High
PossibleDamage: Outdated roles and responsibilities leading to ineffective information security manag
Category: Operational
RiskType: Current
BusinessImpact: Ineffective information security management and increased vulnerability to security th
RiskDescription: Failure to regularly review and update information security roles can lead to gaps in s
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Assign a responsible individual to oversee the review process", "2": "Set a timelin
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1478:
RiskId: 1250
ComplianceId: 1900
RiskTitle: Ineffective Information Security Management Structure
Criticality: High
PossibleDamage: Confusion, inefficiencies, and increased vulnerability to security breaches
Category: Operational
RiskType: Current
BusinessImpact: May result in data breaches, loss of sensitive information, and damage to reputation
RiskDescription: Failure to establish a clear information security management structure may lead to mi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the information security management structure", "2":
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1479:
RiskId: 1251
ComplianceId: 1901
RiskTitle: Unclear Information Security Responsibilities
Criticality: Medium
PossibleDamage: Tasks being overlooked, improper handling of security issues

Category: Operational
RiskType: Current
BusinessImpact: May result in security incidents, data breaches, and regulatory non-compliance
RiskDescription: Failure to assign clear information security responsibilities may lead to confusion, lack
RiskLikelihood: 6
RiskImpact: 6
RiskExposureRating: 36
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Define and communicate responsibilities clearly to all personnel", "2": "Provide reg
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1480:
RiskId: 1252
ComplianceId: 1902
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Risk of unauthorized individuals gaining access to sensitive data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions", "2": "Online training modules", "3": "Knowledge assess
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1481:
RiskId: 1253
ComplianceId: 1903
RiskTitle: RBAC Implementation Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Risk of inadequate access control leading to unauthorized access
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "RBAC policy enforcement", "2": "Regular access reviews", "3": "RBAC training"}
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1482:
RiskId: 1254
ComplianceId: 1904
RiskTitle: Access Review Risk
Criticality: Medium
PossibleDamage: Outdated access rights leading to unauthorized access
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Risk of outdated access rights causing unauthorized access incidents

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular access review schedule", "2": "Automated access review tools", "3": "Acc
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1483:
RiskId: 1255
ComplianceId: 1905
RiskTitle: Phishing Attack Vulnerability
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Employees and contractors lacking awareness of phishing attacks may inadvertently
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular phishing simulation exercises to enhance awareness", "2": "Implement e
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1484:
RiskId: 1256

ComplianceId: 1906
RiskTitle: Evolving Threat Awareness Gap
Criticality: Medium
PossibleDamage: Increased vulnerability to emerging security threats
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Lack of annual training updates may result in employees and contractors being unaw
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update training content based on emerging threats", "2": "Provide real-t
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1485:
RiskId: 1257
ComplianceId: 1907
RiskTitle: Loss of Critical Assets
Criticality: High
PossibleDamage: Loss of critical assets, potential security breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential asset loss
RiskDescription: Failure to conduct comprehensive audits may result in critical assets being misplaced
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular physical audits", "2": "Implement asset tagging and tracking procedures",
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1486:
RiskId: 1258
ComplianceId: 1908
RiskTitle: Software License Non-Compliance
Criticality: Medium
PossibleDamage: Legal consequences, financial penalties
Category: Legal
RiskType: Residual
BusinessImpact: IT department and potentially legal department
RiskDescription: Failure to maintain accurate software license inventory may result in non-compliance
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular software license audits", "2": "Implement software usage monitoring tools
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1487:
RiskId: 1259
ComplianceId: 1909
RiskTitle: Data Breach Due to Misclassified Data
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines

Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Misclassification of sensitive data leading to unauthorized access and data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated data classification tools", "2": "Conduct regular audits of da
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1488:
RiskId: 1260
ComplianceId: 1910
RiskTitle: Data Exposure Due to Lack of Encryption
Criticality: Medium
PossibleDamage: Data leaks, regulatory fines, loss of customer trust
Category: IT
RiskType: Residual
BusinessImpact: Disruption of IT operations, legal consequences
RiskDescription: Sensitive data being exposed during transmission due to lack of encryption
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement end-to-end encryption", "2": "Regularly audit encryption mechanisms",
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1489:
RiskId: 1261
ComplianceId: 1911
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Potential financial losses, reputational damage
RiskDescription: Risk of unauthorized users gaining access to sensitive data and systems
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update user access rights", "2": "Implement strong authentic
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1490:
RiskId: 1262
ComplianceId: 1912
RiskTitle: Weak Authentication Risk
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive data
Category: IT
RiskType: Residual
BusinessImpact: Potential data breaches, loss of sensitive information
RiskDescription: Risk of unauthorized users bypassing weak authentication mechanisms

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update user access rights", "2": "Monitor user access activit
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1491:
RiskId: 1263
ComplianceId: 1913
RiskTitle: Weak Cryptographic Keys
Criticality: High
PossibleDamage: Compromised data leading to unauthorized access
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive information, data breaches
RiskDescription: Using weak cryptographic keys can lead to unauthorized access and compromise the
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Use of industry-standard algorithms and key lengths", "2": "Regular key rotation",
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1492:
RiskId: 1264

ComplianceId: 1914
RiskTitle: Insecure Storage of Cryptographic Keys
Criticality: High
PossibleDamage: Data breaches, unauthorized access to sensitive information
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive information, data breaches
RiskDescription: Insecure storage of cryptographic keys can lead to unauthorized access and compron
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 68
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Centralized key management system with access controls", "2": "Audit trails for ke
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1493:
RiskId: 1265
ComplianceId: 1915
RiskTitle: Key Loss and Data Unavailability
Criticality: Medium
PossibleDamage: Data loss, operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, loss of critical data
RiskDescription: Key loss or unavailability can lead to data loss and operational disruptions, impacting
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 45.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Key escrow mechanisms implementation", "2": "Regular testing of key recovery p
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1494:
RiskId: 1266
ComplianceId: 1916
RiskTitle: Unauthorized Access to Physical Assets
Criticality: High
PossibleDamage: Theft of equipment, compromise of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of assets, reputational damage
RiskDescription: Unauthorized access to physical assets can lead to theft, data breaches, and compro
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update access control systems to address vulnerabilities", "2": "Train er
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1495:
RiskId: 1267
ComplianceId: 1917
RiskTitle: Outdated Access Permissions
Criticality: Medium
PossibleDamage: Unauthorized access to physical assets

Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, loss of assets
RiskDescription: Outdated access permissions can lead to unauthorized access to physical assets, inc
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate access review processes to ensure timely reviews", "2": "Implement rol
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1496:
RiskId: 1268
ComplianceId: 1918
RiskTitle: Unauthorized Visitor Access
Criticality: High
PossibleDamage: Security breaches, theft of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of confidential data, reputational damage
RiskDescription: Visitor gaining access to secure areas without authorization
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access control measures at entry points", "2": "Regularly audit visitor l
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1497:
RiskId: 1269
ComplianceId: 1919
RiskTitle: Unsupervised Visitor Access
Criticality: High
PossibleDamage: Security breaches, theft of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of confidential data, reputational damage
RiskDescription: Visitor accessing restricted areas without supervision
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 69.7
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access control measures at entry points", "2": "Regularly audit visitor e
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1498:
RiskId: 1270
ComplianceId: 1920
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information leading to data breaches and loss of c
Category: Operational
RiskType: Residual
BusinessImpact: Loss of confidential data, reputational damage, regulatory fines
RiskDescription: Risk of unauthorized access to sensitive information by individuals without proper aut

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access control lists", "2": "Provide training on RBAC
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1499:
RiskId: 1271
ComplianceId: 1921
RiskTitle: Unauthorized Access to Critical Systems Risk
Criticality: High
PossibleDamage: Unauthorized access to critical systems and data leading to data breaches and loss
Category: Operational
RiskType: Residual
BusinessImpact: Loss of critical data integrity, reputational damage, regulatory fines
RiskDescription: Risk of unauthorized access to critical systems and data by individuals without proper
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enforce MFA for all critical system access", "2": "Regularly review MFA configurat
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1500:
RiskId: 1272

ComplianceId: 1922
RiskTitle: Failure to Establish Incident Response Team
Criticality: High
PossibleDamage: Delayed or ineffective incident handling, increased impact of security incidents.
Category: Operational
RiskType: Current
BusinessImpact: All business units may suffer financial losses, reputational damage, and regulatory pe
RiskDescription: Failure to establish an incident response team may result in uncoordinated, delayed,
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Define clear roles and responsibilities for team members", "2": "Provide regular tra
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1501:
RiskId: 1273
ComplianceId: 1923
RiskTitle: Failure to Conduct Post-Incident Review
Criticality: Medium
PossibleDamage: Recurring security incidents, unaddressed vulnerabilities, and ineffective incident res
Category: Operational
RiskType: Current
BusinessImpact: All business units may suffer financial losses, reputational damage, and regulatory pe
RiskDescription: Failure to conduct post-incident reviews may lead to recurring security incidents, unad
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Document all findings and recommendations from the review", "2": "Implement ch
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1502:
RiskId: 1274
ComplianceId: 1924
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data exposure, financial losses, reputational damage.
Category: IT
RiskType: Current
BusinessImpact: Loss of customer trust, regulatory fines, legal implications.
RiskDescription: Failure to comply with encryption protocols may lead to data breaches and unauthoriz
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption protocols to latest standards", "2": "Implement multi-f
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1503:
RiskId: 1275
ComplianceId: 1925
RiskTitle: Encryption Key Compromise Risk
Criticality: Medium
PossibleDamage: Data exposure, loss of confidentiality.

Category: IT
RiskType: Current
BusinessImpact: Loss of data integrity, regulatory non-compliance.
RiskDescription: Failure to securely manage encryption keys may result in unauthorized access to sen
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement strong access controls for key management systems", "2": "Regularly
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1504:
RiskId: 1276
ComplianceId: 1926
RiskTitle: Encryption Monitoring Risk
Criticality: High
PossibleDamage: Data breaches, loss of confidentiality.
Category: IT
RiskType: Current
BusinessImpact: Financial losses, reputational damage.
RiskDescription: Failure to monitor encryption configurations may result in undetected vulnerabilities ar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools for encryption configurations", "2": "Condu
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1505:
RiskId: 1277
ComplianceId: 1927
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, leakage of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, legal implications, compliance violations
RiskDescription: Unauthorized access to communication systems can lead to data breaches and leaka
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access control lists", "2": "Conduct periodic access c
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1506:
RiskId: 1278
ComplianceId: 1928
RiskTitle: Multi-Factor Authentication Risk
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access to sensitive communication channels
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, compliance violations
RiskDescription: Lack of multi-factor authentication for sensitive communication channels can lead to u

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update access control lists", "2": "Conduct periodic access c
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1507:
RiskId: 1279
ComplianceId: 1929
RiskTitle: Access Control Policy Risk
Criticality: High
PossibleDamage: Data breaches, unauthorized access
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, compliance violations
RiskDescription: Inadequate access control policies can lead to unauthorized access, data breaches, a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access control lists", "2": "Conduct periodic access c
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1508:
RiskId: 1280

ComplianceId: 1930
RiskTitle: Failure to Develop Secure Coding Standards
Criticality: High
PossibleDamage: Increased vulnerability to security breaches and data loss
Category: Operational
RiskType: Inherent
BusinessImpact: Development delays, reputational damage, financial losses
RiskDescription: Failure to establish secure coding standards may lead to the introduction of vulnerabil
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update coding standards based on emerging threats", "2": "Provide ong
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1509:
RiskId: 1281
ComplianceId: 1931
RiskTitle: Lack of Training on Secure Coding Practices
Criticality: Medium
PossibleDamage: Developers not following secure coding practices, leading to security vulnerabilities
Category: Operational
RiskType: Inherent
BusinessImpact: Data breaches, reputational damage
RiskDescription: Failure to provide training on secure coding practices may result in developers not foll
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly conduct refresher training sessions", "2": "Provide access to resources

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Retail Banking

Item 1510:

RiskId: 1282

ComplianceId: 1932

RiskTitle: Failure to Conduct Code Reviews and Analysis

Criticality: High

PossibleDamage: Undetected security vulnerabilities in the code

Category: Operational

RiskType: Inherent

BusinessImpact: Data breaches, financial losses

RiskDescription: Failure to conduct code reviews and analysis may result in undetected security vulner

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish a regular schedule for code reviews and analysis", "2": "Implement auto

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1511:

RiskId: 1283

ComplianceId: 1933

RiskTitle: Failure to Identify Critical Suppliers

Criticality: High

PossibleDamage: Inadequate security assessments and potential security breaches

Category: Operational
RiskType: Inherent
BusinessImpact: Data breaches, service disruptions, reputational damage
RiskDescription: Failure to identify critical suppliers may result in inadequate security assessments, ex
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a supplier risk assessment framework", "2": "Regularly review and upd
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1512:
RiskId: 1284
ComplianceId: 1934
RiskTitle: Failure to Conduct Regular Security Assessments on Suppliers
Criticality: Medium
PossibleDamage: Unidentified security vulnerabilities in the supply chain
Category: Operational
RiskType: Inherent
BusinessImpact: Data breaches, service disruptions
RiskDescription: Failure to conduct regular security assessments on suppliers may result in unidentifie
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a regular assessment schedule for suppliers", "2": "Automate assessme
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1513:
RiskId: 1285
ComplianceId: 1935
RiskTitle: Failure to Include Minimum Security Requirements in Supplier Contracts
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, legal liabilities
Category: Operational
RiskType: Current
BusinessImpact: All business units would be impacted by potential data breaches and legal liabilities
RiskDescription: Failure to include minimum security requirements in supplier contracts may result in d
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Review and negotiate contract terms with suppliers to ensure alignment with secu
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1514:
RiskId: 1286
ComplianceId: 1936
RiskTitle: Failure to Specify Supplier Responsibilities for Security Incident Reporting and Resolution
Criticality: Medium
PossibleDamage: Delayed incident response, increased impact of security breaches, regulatory non-c
Category: Operational
RiskType: Current
BusinessImpact: All business units would be impacted by delayed incident response and security brea
RiskDescription: Failure to specify supplier responsibilities for security incident reporting and resolution

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Obtain legal review and approval of contract terms related to security obligations"
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1515:
RiskId: 1287
ComplianceId: 1937
RiskTitle: Undetected Security Breaches
Criticality: High
PossibleDamage: Data theft, system compromise
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, damage to reputation
RiskDescription: Failure to monitor security logs and alerts may result in undetected security breaches
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools", "2": "Train staff on identifying security inc
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1516:
RiskId: 1288

ComplianceId: 1938
RiskTitle: System Vulnerabilities Exploited
Criticality: Medium
PossibleDamage: Data breaches, system downtime
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, disruption of operations
RiskDescription: Failure to conduct periodic vulnerability assessments may result in unaddressed vuln
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated vulnerability scanning tools", "2": "Establish patch manager
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1517:
RiskId: 1289
ComplianceId: 1939
RiskTitle: Ineffective Incident Response
Criticality: Low
PossibleDamage: Repeated incidents, ineffective response
Category: IT
RiskType: Residual
BusinessImpact: Increased incident resolution time, potential escalation of incidents
RiskDescription: Failure to document security incidents may result in ineffective incident response and
RiskLikelihood: 4
RiskImpact: 3
RiskExposureRating: 12
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Low

RiskMitigation: {"1": "Implement incident tracking system", "2": "Train staff on incident documentation p

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 1518:

RiskId: 1290

ComplianceId: 1940

RiskTitle: Delayed Incident Reporting

Criticality: High

PossibleDamage: Increased impact of security incidents

Category: Operational

RiskType: Residual

BusinessImpact: Delayed incident response, potential data breaches, financial losses, and reputationa

RiskDescription: Failure to report incidents promptly may result in delayed response and increased imp

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Provide regular training on incident reporting procedures", "2": "Implement automa

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1519:

RiskId: 1291

ComplianceId: 1941

RiskTitle: Inadequate Incident Documentation

Criticality: Medium

PossibleDamage: Repeated incidents, inability to track trends

Category: Operational
RiskType: Residual
BusinessImpact: Inability to track incident trends, repeated incidents, and ineffective incident response
RiskDescription: Lack of documentation may lead to repeated incidents or inability to track trends.
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement incident tracking system", "2": "Regularly review incident documentatio
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1520:
RiskId: 1292
ComplianceId: 1942
RiskTitle: Miscommunication within Incident Response Team
Criticality: High
PossibleDamage: Delays in incident response and increased impact
Category: Operational
RiskType: Current
BusinessImpact: Delays in incident response could lead to prolonged downtime and increased damage
RiskDescription: Lack of clear roles and responsibilities within the incident response team could result
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for team members to understand their roles", "2": "Esta
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1521:
RiskId: 1293
ComplianceId: 1943
RiskTitle: Inadequate Preparedness for Incidents
Criticality: Medium
PossibleDamage: Ineffective response and increased damage
Category: Operational
RiskType: Current
BusinessImpact: Ineffective response could lead to prolonged downtime and increased damage
RiskDescription: Failure to conduct regular incident response plan exercises may result in inadequate
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly schedule tabletop exercises to simulate various incident scenarios", "2"
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1522:
RiskId: 1294
ComplianceId: 1944
RiskTitle: Failure to Conduct BIA
Criticality: High
PossibleDamage: Financial losses, operational downtime, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to conduct BIA may lead to unpreparedness for disruptions, resulting in financ

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the BIA findings", "2": "Conduct periodic drills to test
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1523:
RiskId: 1295
ComplianceId: 1945
RiskTitle: Failure to Review and Update BIA Annually
Criticality: Medium
PossibleDamage: Inaccurate risk assessments, ineffective response strategies
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Outdated BIA findings may lead to inaccurate risk assessments and ineffective respo
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a regular review schedule for BIA updates", "2": "Include new business
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1524:
RiskId: 1296

ComplianceId: 1946
RiskTitle: Ineffective BCP Team
Criticality: High
PossibleDamage: Increased downtime, financial losses
Category: Operational
RiskType: Current
BusinessImpact: All business units would face disruptions and financial losses
RiskDescription: Failure to establish a dedicated BCP team may result in delays in response to disrupt
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and updates for the team", "2": "Ensuring clear roles and respons
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1525:
RiskId: 1297
ComplianceId: 1947
RiskTitle: Ineffective BCP Testing
Criticality: High
PossibleDamage: Ineffective response during disruptions, financial losses
Category: Operational
RiskType: Current
BusinessImpact: All business units would face disruptions and financial losses
RiskDescription: Failure to test the BCP regularly may result in ineffective response during actual disru
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular testing schedule and documentation", "2": "Involvement of key stakehold

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1526:

RiskId: 1298

ComplianceId: 1948

RiskTitle: Non-Compliance with Legal and Regulatory Requirements

Criticality: High

PossibleDamage: Potential fines, legal actions, reputational damage, and loss of business opportunitie

Category: Compliance

RiskType: Current

BusinessImpact: Legal and financial consequences affecting all business units

RiskDescription: Failure to comply with legal and regulatory requirements may result in legal actions, fi

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update the requirements register", "2": "Provide training on new require

CreatedAt: 2025-10-11 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1527:

RiskId: 1299

ComplianceId: 1949

RiskTitle: Non-Compliance Identified During Quarterly Reviews

Criticality: Medium

PossibleDamage: Potential legal actions, fines, reputational damage, and loss of business opportunitie

Category: Compliance
RiskType: Current
BusinessImpact: Legal and financial consequences affecting all business units
RiskDescription: Identification of non-compliance issues during quarterly reviews may result in legal ac
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Assign a compliance officer to oversee monitoring activities", "2": "Implement regu
CreatedAt: 2025-10-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1528:
RiskId: 860
ComplianceId: 876
RiskTitle: Unauthorized Access Due to Role Changes
Criticality: High
PossibleDamage: Unauthorized access to sensitive information or systems
Category: Operational
RiskType: Residual
BusinessImpact: Potential data breaches, loss of intellectual property, or financial loss
RiskDescription: Failure to re-authenticate users after role changes may lead to unauthorized access t
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access controls", "2": "Regularly review and update user ro
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1529:
RiskId: 861
ComplianceId: 877
RiskTitle: Session Hijacking and Unauthorized Access
Criticality: Medium
PossibleDamage: Session hijacking, unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Potential data breaches, loss of sensitive information, reputational damage
RiskDescription: Failure to re-authenticate users after a fixed time period may lead to session hijacking
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement session timeout policies", "2": "Educate users on the importance of log
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1530:
RiskId: 862
ComplianceId: 878
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information and potential data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, reputational damage, and financial losses
RiskDescription: Risk of unauthorized individuals gaining access to organizational systems and sensitiv

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for all user accounts", "2": "Regularly review
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1531:
RiskId: 863
ComplianceId: 879
RiskTitle: Identity Resolution Risk
Criticality: Medium
PossibleDamage: Identity fraud, misuse of user accounts, and potential legal issues
Category: Legal
RiskType: Residual
BusinessImpact: Potential legal liabilities, reputational damage, and financial losses
RiskDescription: Risk of unresolved user identities leading to identity fraud, misuse of user accounts, a
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement identity verification processes for all new user accounts", "2": "Regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1532:
RiskId: 864

ComplianceId: 880
RiskTitle: Identity Evidence Collection Risk
Criticality: High
PossibleDamage: Inaccurate user credentials, potential security breaches, and legal issues
Category: Operational
RiskType: Residual
BusinessImpact: Potential security breaches, legal liabilities, reputational damage, and financial losses
RiskDescription: Risk of inaccurate user credentials, security breaches, and legal issues due to improp
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated identity verification tools", "2": "Train employees on proper
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1533:
RiskId: 865
ComplianceId: 881
RiskTitle: Unauthorized Access Due to Fraudulent Identification
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, identity theft
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to verify identity evidence may lead to unauthorized access and potential data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for added security", "2": "Regularly update a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1534:
RiskId: 866
ComplianceId: 882
RiskTitle: Biometric Verification Failure
Criticality: Critical
PossibleDamage: Unauthorized access to critical systems, data breaches, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Sensitive business units
RiskDescription: Failure of biometric verification systems may result in unauthorized access to critical s
RiskLikelihood: 7
RiskImpact: 10
RiskExposureRating: 70
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update biometric systems and algorithms", "2": "Conduct regular trainin
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1535:
RiskId: 867
ComplianceId: 883
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Financial loss, reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: Unauthorized access to sensitive information could lead to financial loss and reputatio
RiskDescription: Unauthorized access to sensitive information by malicious actors due to inadequate id
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication mechanisms", "2": "Regularly audit access logs f
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1536:
RiskId: 868
ComplianceId: 884
RiskTitle: Identity Fraud and Account Takeover
Criticality: Medium
PossibleDamage: Financial loss, data breaches
Category: Financial
RiskType: Residual
BusinessImpact: Identity fraud and account takeover could lead to financial loss and data breaches
RiskDescription: Unauthorized individuals gaining access to sensitive information through fraudulent id
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement biometric authentication for sensitive accounts", "2": "Regularly update
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1537:
RiskId: 869
ComplianceId: 885
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of confidential data, reputation damage
RiskDescription: Failure to confirm user address may lead to unauthorized individuals gaining access t
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for additional security", "2": "Regularly revie
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1538:
RiskId: 870
ComplianceId: 886
RiskTitle: Ineffective Incident Response Policy Implementation
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units affected by security incidents
RiskDescription: Failure to implement an effective incident response policy may result in delayed respo

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Training on policy implementation", "3"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1539:
RiskId: 871
ComplianceId: 887
RiskTitle: Lack of Designated Incident Response Policy Official
Criticality: Medium
PossibleDamage: Confusion, delays, inconsistencies in policy management
Category: Operational
RiskType: Residual
BusinessImpact: All business units affected by inconsistent policy implementation
RiskDescription: Failure to designate an official to manage incident response policy may result in confu
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear role description and responsibilities", "2": "Regular performance reviews for
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1540:
RiskId: 872

ComplianceId: 888
RiskTitle: Outdated Incident Response Policy
Criticality: High
PossibleDamage: Ineffective incident response, increased security risks, non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: All business units affected by security incidents
RiskDescription: Failure to review and update the incident response policy may result in outdated proc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Incident response drills and simulation
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1541:
RiskId: 873
ComplianceId: 889
RiskTitle: Inadequate Incident Response Training
Criticality: High
PossibleDamage: Delayed incident response, increased impact of incidents, potential data breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units may experience disruptions and financial losses
RiskDescription: Failure to provide adequate incident response training may result in ineffective incide
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly review and update incident response training content", "2": "Conduct pe

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 1542:

RiskId: 874

ComplianceId: 890

RiskTitle: Ineffective Incident Response Capability

Criticality: High

PossibleDamage: Data breaches, system downtime, financial losses

Category: Operational

RiskType: Current

BusinessImpact: Disruption of operations, loss of sensitive data, financial repercussions

RiskDescription: Failure to effectively respond to incidents can result in data breaches, system downtin

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly test incident response capabilities", "2": "Update incident response proc

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1543:

RiskId: 875

ComplianceId: 891

RiskTitle: Ineffective Incident Response Coordination

Criticality: High

PossibleDamage: Extended downtime, data loss, and reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: Delays in response and recovery, increased operational costs
RiskDescription: Failure to coordinate incident response testing with related plans may lead to ineffecti
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular communication and collaboration between teams responsible for incident
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1544:
RiskId: 876
ComplianceId: 892
RiskTitle: Failure to Implement Incident Handling Capability
Criticality: High
PossibleDamage: Prolonged security incidents, data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to implement an incident handling capability may lead to ineffective incident re
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and testing of incident response procedures", "2": "Continuous m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1545:
RiskId: 877
ComplianceId: 893
RiskTitle: Lack of Coordination between Incident Handling and Contingency Planning
Criticality: Medium
PossibleDamage: Ineffective response during critical incidents, increased downtime
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Lack of coordination between incident handling and contingency planning may lead to
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular joint exercises and drills between incident handling and contingency plan
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1546:
RiskId: 878
ComplianceId: 894
RiskTitle: Inadequate Incident Response
Criticality: High
PossibleDamage: Data breaches, system downtime, and reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, and loss of customer trust
RiskDescription: Failure to utilize online incident management systems may result in delayed incident r

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on system usage", "2": "Continuous monitoring of system perform
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1547:
RiskId: 879
ComplianceId: 895
RiskTitle: Incomplete Forensic Analysis
Criticality: Medium
PossibleDamage: Inability to identify root causes of incidents and prevent future occurrences
Category: IT
RiskType: Residual
BusinessImpact: Increased vulnerability to security threats and potential data breaches
RiskDescription: Failure to implement full network packet capture may result in incomplete forensic ana
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular testing of packet capture systems", "2": "Continuous monitoring of networ
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1548:
RiskId: 880

ComplianceId: 896
RiskTitle: Incomplete Incident Documentation
Criticality: High
PossibleDamage: Increased risk exposure, delayed incident response, and compromised security post
Category: Operational
RiskType: Residual
BusinessImpact: Potential security breaches, data loss, and reputational damage
RiskDescription: Failure to document incidents accurately and comprehensively may lead to misinterpr
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated incident tracking systems", "2": "Provide training on inciden
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1549:
RiskId: 881
ComplianceId: 897
RiskTitle: Inadequate Incident Analysis
Criticality: Medium
PossibleDamage: Recurring incidents, undetected vulnerabilities, and ineffective incident response stra
Category: Operational
RiskType: Residual
BusinessImpact: Increased incident response times, higher incident resolution costs, and compromised
RiskDescription: Lack of proactive incident analysis may lead to recurring incidents, undetected vulnera
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement incident analysis tools and techniques", "2": "Conduct regular incident
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1550:
RiskId: 882
ComplianceId: 898
RiskTitle: Delayed Incident Reporting
Criticality: High
PossibleDamage: Increased impact and severity of incidents
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches, operational disruptions
RiskDescription: Failure to report incidents within the specified time frame may result in delayed incide
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated incident reporting systems", "2": "Provide regular training o
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1551:
RiskId: 883
ComplianceId: 899
RiskTitle: Failure to Report to Designated Authorities
Criticality: Medium
PossibleDamage: Inadequate response and resolution of incidents

Category: Operational
RiskType: Current
BusinessImpact: Prolonged incidents, increased risk exposure
RiskDescription: Not reporting incident information to designated authorities within the specified time fr
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting channels and escalation procedures", "2": "Conduct regu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1552:
RiskId: 884
ComplianceId: 900
RiskTitle: Failure to Report Incidents Timely and Accurately
Criticality: High
PossibleDamage: Legal consequences, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Delayed incident response, increased severity of incidents, potential legal implications
RiskDescription: Failure to report incidents through automated mechanisms may lead to delayed respo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on automated reporting tools", "2": "Periodic testing of automated
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1553:
RiskId: 885
ComplianceId: 901
RiskTitle: Failure to Report Supply Chain Incidents
Criticality: High
PossibleDamage: Delays in incident resolution, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Disruption of supply chain operations, loss of customer trust
RiskDescription: Not reporting supply chain incidents can lead to prolonged disruptions, financial losse
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear incident reporting procedures", "2": "Regular training for staff on in
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1554:
RiskId: 886
ComplianceId: 902
RiskTitle: Inadequate Incident Response Support Resource
Criticality: High
PossibleDamage: Delayed incident response, increased impact of incidents, and potential data breach
Category: Operational
RiskType: Current
BusinessImpact: Delays in incident response, potential data breaches, and reputational damage
RiskDescription: Failure to establish a robust incident response support resource may lead to inefficien

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for support staff on incident response procedures", "2": "Regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1555:
RiskId: 887
ComplianceId: 903
RiskTitle: Inadequate Incident Response Plan
Criticality: High
PossibleDamage: Delayed incident response, increased impact on the organization, potential regulator
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be affected by incidents resulting from inadequate planning
RiskDescription: Failure to develop a comprehensive incident response plan may lead to delayed respo
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of the incident response plan", "2": "Training and awar
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1556:
RiskId: 888

ComplianceId: 904
RiskTitle: Lack of Incident Response Plan Distribution
Criticality: Medium
PossibleDamage: Lack of awareness among key personnel, leading to ineffective incident response
Category: Operational
RiskType: Residual
BusinessImpact: All business units could be affected by delays in incident response
RiskDescription: Failure to distribute the incident response plan may result in lack of awareness among
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a distribution process with clear responsibilities and timelines", "2": "Pro
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1557:
RiskId: 889
ComplianceId: 905
RiskTitle: Delayed Response to Information Spillage
Criticality: High
PossibleDamage: Data breaches, reputational damage, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, damage to reputation, financial penalties
RiskDescription: Failure to assign responsible personnel for information spillage response may result i
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on information spillage response proce
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1558:
RiskId: 890
ComplianceId: 906
RiskTitle: Failure to Isolate Contaminated System
Criticality: Medium
PossibleDamage: Spread of sensitive information to unauthorized systems, data exposure risks
Category: IT
RiskType: Current
BusinessImpact: Data exposure, potential regulatory fines
RiskDescription: Lack of proper isolation of contaminated systems may lead to the inadvertent spread
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated system monitoring for detecting information spills", "2": "Establish clea
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1559:
RiskId: 891
ComplianceId: 907
RiskTitle: Inadequate Information Spillage Response Training
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, legal liabilities
RiskDescription: Lack of proper training may result in personnel not knowing how to respond to informa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for all personnel", "2": "Simulated drills to test response
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1560:
RiskId: 892
ComplianceId: 908
RiskTitle: Disruption of Organizational Operations
Criticality: High
PossibleDamage: Operational delays and potential financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Personnel unable to perform critical tasks due to contaminated systems, leading to op
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide alternative systems or workarounds for affected personnel", "2": "Ensure
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1561:
RiskId: 893
ComplianceId: 909
RiskTitle: Legal Consequences of Information Spillage
Criticality: High
PossibleDamage: Legal penalties, reputation damage, financial losses
Category: Legal
RiskType: Current
BusinessImpact: Legal actions, fines, loss of credibility
RiskDescription: Failure to comply with information spillage laws can result in legal actions, fines, and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Legal compliance training for all employees", "2": "Strict enforcement of informatio
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1562:
RiskId: 894
ComplianceId: 910
RiskTitle: Data Breach Due to Unauthorized Exposure
Criticality: Medium
PossibleDamage: Data breaches, loss of intellectual property, regulatory fines
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive data, regulatory penalties, damage to reputation
RiskDescription: Unauthorized exposure to sensitive information can lead to data breaches, loss of inte

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement access controls for sensitive information", "2": "Regular monitoring of a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1563:
RiskId: 895
ComplianceId: 911
RiskTitle: Inadequate Maintenance Policy Implementation
Criticality: High
PossibleDamage: Increased security risks, legal penalties, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential disruption of operations, financial losses, and damage to organizational repu
RiskDescription: Failure to implement a comprehensive maintenance policy may result in unauthorized
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Continuous monitoring of maintenance
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1564:
RiskId: 896

ComplianceId: 912
RiskTitle: Lack of Designated Maintenance Policy Official
Criticality: Medium
PossibleDamage: Confusion, delays, and inconsistencies in policy management
Category: Operational
RiskType: Current
BusinessImpact: Potential delays in policy development, mismanagement of procedures, and lack of o
RiskDescription: Failure to designate an official for maintenance policy management may result in conf
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clearly define roles and responsibilities of the designated official", "2": "Provide ne
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1565:
RiskId: 897
ComplianceId: 913
RiskTitle: Outdated Maintenance Policy and Procedures
Criticality: High
PossibleDamage: Ineffective maintenance practices, increased security vulnerabilities, and non-compli
Category: Operational
RiskType: Current
BusinessImpact: Potential security breaches, data loss, and legal consequences
RiskDescription: Failure to review and update maintenance policy and procedures may result in outdat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear review schedules for policies and procedures", "2": "Engage stake
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1566:
RiskId: 898
ComplianceId: 914
RiskTitle: Incomplete Maintenance Records
Criticality: High
PossibleDamage: System downtime, Security breaches
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, Data loss
RiskDescription: Failure to maintain accurate records of maintenance activities may result in improper
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a centralized maintenance tracking system", "2": "Regularly audit mair
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1567:
RiskId: 899
ComplianceId: 915
RiskTitle: Unauthorized Off-Site Maintenance
Criticality: Medium
PossibleDamage: Data breaches, Unauthorized access

Category: Legal
RiskType: Current
BusinessImpact: Legal penalties, Reputation damage
RiskDescription: Unauthorized removal of system components for off-site maintenance may result in d
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a formal approval process for off-site maintenance", "2": "Track and m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1568:
RiskId: 900
ComplianceId: 916
RiskTitle: Unauthorized Use of Maintenance Tools
Criticality: High
PossibleDamage: Data breaches, system downtime, financial losses
Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, loss of sensitive data, financial penalties
RiskDescription: Unauthorized maintenance tools could introduce vulnerabilities and malicious code in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on approved maintenance tools", "2": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1569:
RiskId: 901
ComplianceId: 917
RiskTitle: Compromised Maintenance Tools
Criticality: High
PossibleDamage: System compromise, data breach, operational disruptions
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of maintenance operations, loss of sensitive data, financial losses
RiskDescription: Unauthorized modifications in maintenance tools could lead to the installation of malic
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular inspection and monitoring of maintenance tools", "2": "Implementing acce
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1570:
RiskId: 902
ComplianceId: 918
RiskTitle: Malicious Code Introduction
Criticality: High
PossibleDamage: System compromise, data loss, operational disruptions
Category: IT
RiskType: Inherent
BusinessImpact: Significant impact on IT operations, data security, and system availability
RiskDescription: Introduction of malicious code through unchecked media can lead to malware infectio

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update antivirus software", "2": "Implement media scanning policies", "3
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1571:
RiskId: 903
ComplianceId: 919
RiskTitle: Data Breach due to Unauthorized Removal of Maintenance Equipment
Criticality: High
PossibleDamage: Loss of sensitive organizational information, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Unauthorized removal of maintenance equipment containing organizational informatio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls for maintenance equipment", "2": "Regularly mon
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1572:
RiskId: 904

ComplianceId: 920
RiskTitle: Data Leakage from Improperly Disposed Maintenance Equipment
Criticality: Medium
PossibleDamage: Loss of sensitive data, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Legal consequences, reputational damage
RiskDescription: Improper disposal of maintenance equipment containing organizational information co
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement secure disposal procedures for equipment", "2": "Train employees on p
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1573:
RiskId: 905
ComplianceId: 921
RiskTitle: Unauthorized Access to Systems
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Unauthorized individuals gaining access to critical systems and data through nonloca
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication measures", "2": "Regularly review access logs fo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1574:
RiskId: 906
ComplianceId: 922
RiskTitle: Weak Authentication for Nonlocal Maintenance
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Data security, IT operations
RiskDescription: Unauthorized individuals gaining access to systems due to weak authentication mech
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement multi-factor authentication for nonlocal maintenance sessions", "2": "U
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1575:
RiskId: 907
ComplianceId: 923
RiskTitle: Lack of Maintenance Activity Records
Criticality: Low
PossibleDamage: Inability to trace unauthorized access, lack of accountability

Category: Operational
RiskType: Residual
BusinessImpact: Data security, IT operations
RiskDescription: Inability to track and monitor nonlocal maintenance activities, leading to potential unau
RiskLikelihood: 4
RiskImpact: 3
RiskExposureRating: 12
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Implement logging mechanisms for nonlocal maintenance activities", "2": "Regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1576:
RiskId: 908
ComplianceId: 924
RiskTitle: Unauthorized Access by Maintenance Personnel
Criticality: High
PossibleDamage: System compromise, data breach, operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Loss of data, system downtime, reputational damage
RiskDescription: Unauthorized maintenance personnel gaining access to critical systems can lead to d
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the list of authorized maintenance personnel", "2": "I
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1577:
RiskId: 909
ComplianceId: 925
RiskTitle: Unauthorized Access by Non-Escorted Personnel
Criticality: Medium
PossibleDamage: System compromise, operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, potential financial losses
RiskDescription: Non-escorted personnel without required access authorizations gaining access to criti
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement access control measures to restrict unauthorized access", "2": "Regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1578:
RiskId: 910
ComplianceId: 926
RiskTitle: Lack of Supervision in Maintenance Activities
Criticality: High
PossibleDamage: Unauthorized access, system compromise
Category: Operational
RiskType: Current
BusinessImpact: Data breaches, operational disruptions
RiskDescription: Inadequate supervision during maintenance activities can lead to unauthorized acces

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training to supervising personnel on security protocols and access contro
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1579:
RiskId: 911
ComplianceId: 927
RiskTitle: Unauthorized Access by Maintenance Personnel
Criticality: High
PossibleDamage: Unauthorized access to classified information leading to data breaches or leaks
Category: Operational
RiskType: Residual
BusinessImpact: IT, Security, Operations
RiskDescription: Risk of maintenance personnel without appropriate security clearances gaining acces
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict escort and supervision protocols for maintenance personnel", "2"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1580:
RiskId: 912

ComplianceId: 928
RiskTitle: Lack of Sanitization Before Maintenance Activities
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information due to lack of sanitization
Category: IT
RiskType: Residual
BusinessImpact: IT, Security, Operations
RiskDescription: Risk of maintenance personnel gaining unauthorized access to sensitive information d
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement strict sanitization procedures for information system components", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1581:
RiskId: 913
ComplianceId: 929
RiskTitle: Lack of Alternate Security Safeguards for Unsanitizable Components
Criticality: High
PossibleDamage: Risk of unauthorized access to sensitive information due to lack of alternate security
Category: IT
RiskType: Residual
BusinessImpact: IT, Security, Operations
RiskDescription: Risk of unauthorized access to sensitive information due to lack of alternate security s
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Develop and implement encryption mechanisms for unsanitizable components", "

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1582:

RiskId: 914

ComplianceId: 930

RiskTitle: Extended Downtime and Data Loss

Criticality: High

PossibleDamage: Extended downtime, loss of critical data, financial losses

Category: Operational

RiskType: Current

BusinessImpact: Significant impact on operations, financial losses, and potential damage to organizati

RiskDescription: Failure to obtain timely maintenance support for critical system components can lead

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish contracts with maintenance providers for quick response times", "2": "Im

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1583:

RiskId: 915

ComplianceId: 931

RiskTitle: Unauthorized Access to Sensitive Media

Criticality: High

PossibleDamage: Data breaches, loss of sensitive information, legal consequences

Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Unauthorized access to sensitive media can result in data breaches, loss of confident
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls", "2": "Encrypt sensitive media", "3": "Regular security
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1584:
RiskId: 916
ComplianceId: 932
RiskTitle: Inconsistent Policy Implementation
Criticality: Medium
PossibleDamage: Policy inconsistencies, lack of oversight, increased security risks
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Lack of a designated official for managing media protection policy may result in incons
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear role definition and responsibilities", "2": "Regular reporting and updates to m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 1585:
RiskId: 917
ComplianceId: 933
RiskTitle: Outdated Policies and Procedures
Criticality: High
PossibleDamage: Ineffective controls, increased security vulnerabilities, non-compliance
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Outdated media protection policies and procedures can result in ineffective controls, i
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy and procedure reviews", "2": "Incident response planning", "3": "Tr
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1586:
RiskId: 918
ComplianceId: 934
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, privacy violations, intellectual property theft
Category: Compliance
RiskType: Residual
BusinessImpact: Loss of trust, legal repercussions, financial losses
RiskDescription: Unauthorized access to patient medical records or design specifications could lead to

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access controls for digital and non-digital media", "2": "Reg
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1587:
RiskId: 919
ComplianceId: 937
RiskTitle: Unauthorized Access to System Media
Criticality: High
PossibleDamage: Unauthorized access to sensitive information stored on system media, potential data
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive information, potential legal and financial implications
RiskDescription: Unauthorized individuals gaining access to system media containing sensitive informa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls to restricted areas where media is stored", "2": "Regul
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1588:
RiskId: 920

ComplianceId: 938
RiskTitle: Unauthorized Access to Sensitive Information After Media Disposal
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information after media disposal, potential data lea
Category: Operational
RiskType: Current
BusinessImpact: Potential data leaks, compliance violations
RiskDescription: Sensitive information stored on system media being accessed by unauthorized indivic
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement secure disposal procedures for system media", "2": "Use approved equ
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1589:
RiskId: 921
ComplianceId: 940
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Unauthorized disclosure of sensitive information leading to data breaches and comp
Category: Compliance
RiskType: Residual
BusinessImpact: All business units would be impacted by potential data breaches and compliance viol
RiskDescription: Risk of unauthorized disclosure of sensitive information due to improper media sanitiz
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls for media sanitization processes", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1590:
RiskId: 922
ComplianceId: 941
RiskTitle: Unauthorized Access Risk
Criticality: Medium
PossibleDamage: Inadequate sanitization leading to unauthorized access to sensitive information
Category: Compliance
RiskType: Residual
BusinessImpact: All business units would be impacted by potential unauthorized access to sensitive in
RiskDescription: Risk of unauthorized access to sensitive information due to inadequate sanitization m
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement data classification policies to determine appropriate sanitization mecha
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1591:
RiskId: 923
ComplianceId: 942
RiskTitle: Data Breach due to Unauthorized System Media Use
Criticality: High
PossibleDamage: Data breaches can result in financial losses, reputational damage, and legal conseq

Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive information, regulatory fines, damage to reputation
RiskDescription: Unauthorized use of system media can lead to data breaches where sensitive informa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls to restrict use of system media based on user roles", "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1592:
RiskId: 924
ComplianceId: 943
RiskTitle: Malware Infection from Unowned Portable Storage Devices
Criticality: Medium
PossibleDamage: Malware infections can disrupt operations, lead to data loss, and compromise syster
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, potential data loss, compromised system security
RiskDescription: Use of portable storage devices without identifiable owner can introduce malware into
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement endpoint security solutions to monitor and control portable storage dev
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1593:
RiskId: 925
ComplianceId: 944
RiskTitle: Unauthorized Access and Compromise of Physical Security Measures
Criticality: High
PossibleDamage: Unauthorized access to sensitive information and physical security breaches
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of sensitive data, damage to reputation
RiskDescription: Failure to comply with physical and environmental protection policy may lead to unaut
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls and monitoring systems", "2": "Regular security asses
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 1594:
RiskId: 926
ComplianceId: 945
RiskTitle: Confusion and Inconsistency in Policy Management
Criticality: Medium
PossibleDamage: Confusion, inconsistency, and non-compliance with policies
Category: Operational
RiskType: Residual
BusinessImpact: Inefficiencies in policy implementation, increased risk of non-compliance
RiskDescription: Failure to designate an official for policy management may lead to confusion, inconsis

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear role definition and responsibilities for the official", "2": "Regular reporting an
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1595:
RiskId: 927
ComplianceId: 946
RiskTitle: Non-Compliance and Security Incidents Due to Outdated Policies
Criticality: High
PossibleDamage: Vulnerabilities, non-compliance, legal liabilities, and security incidents
Category: Operational
RiskType: Residual
BusinessImpact: Legal consequences, financial penalties, reputational damage
RiskDescription: Failure to review and update policies and procedures may result in non-compliance w
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy review cycles and updates", "2": "Incident-driven updates based o
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1596:
RiskId: 928

ComplianceId: 947
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive areas leading to data breaches or physical security
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of sensitive data, compromised physical security, reputational damage.
RiskDescription: Risk of unauthorized individuals gaining access to restricted areas within the facility, p
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of access lists", "2": "Implement two-factor authentication for acces
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1597:
RiskId: 929
ComplianceId: 948
RiskTitle: Outdated Access List Risk
Criticality: Medium
PossibleDamage: Outdated access lists leading to unauthorized access or delays in access removal.
Category: Operational
RiskType: Inherent
BusinessImpact: Unauthorized access, security incidents, potential data breaches.
RiskDescription: Risk of outdated access lists resulting in unauthorized individuals retaining access or
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Automate access list reviews", "2": "Implement access expiration dates", "3": "Enf
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1598:
RiskId: 930
ComplianceId: 949
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive areas, theft, data breaches
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, disruption of operations, financial losses
RiskDescription: Unauthorized individuals gaining access to restricted areas can lead to theft of physic
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access control measures", "2": "Regularly review and update acc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1599:
RiskId: 931
ComplianceId: 950
RiskTitle: Audit Log Maintenance Risk
Criticality: Medium
PossibleDamage: Lack of visibility into access activities, inability to trace unauthorized access

Category: Operational
RiskType: Current
BusinessImpact: Inability to trace unauthorized access, compliance violations, security incidents
RiskDescription: Failure to maintain audit logs can result in lack of visibility into access activities, makir
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review audit logs for anomalies", "2": "Implement automated monitoring
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1600:
RiskId: 932
ComplianceId: 951
RiskTitle: Unauthorized Access to System Distribution and Transmission Lines
Criticality: High
PossibleDamage: Data breaches, communication disruptions, and potential tampering with sensitive in
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of confidential data, interruptions in communication, and damage to org
RiskDescription: Unauthorized individuals gaining access to system distribution and transmission lines
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access control mechanisms such as card readers or biometric scanne
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1601:
RiskId: 933
ComplianceId: 952
RiskTitle: Data Breach Due to Unauthorized Access to Output Devices
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, and compromised security
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties, and reputational damage
RiskDescription: Unauthorized individuals gaining access to output devices can lead to data breaches,
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security audits of output device access controls", "2": "Employee training
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1602:
RiskId: 934
ComplianceId: 953
RiskTitle: Unauthorized Access to Facilities
Criticality: High
PossibleDamage: Data breaches, theft, or physical harm to individuals.
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, financial losses, damage to reputation.
RiskDescription: Unauthorized access to facilities can lead to breaches of physical security, compromis

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access control measures like key cards or biometric scanners", "2": "R
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1603:
RiskId: 935
ComplianceId: 954
RiskTitle: Failure to Detect Security Incidents
Criticality: Medium
PossibleDamage: Breaches or unauthorized access due to undetected threats.
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, financial losses, damage to reputation.
RiskDescription: Failure to review access logs regularly may result in undetected security incidents, lea
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate log review processes to ensure timely detection", "2": "Implement anom
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1604:
RiskId: 936

ComplianceId: 955
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Theft, vandalism, or compromise of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of assets, damage to property, or data breach incidents.
RiskDescription: Unauthorized individuals gaining access to the facility can lead to various security bre
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security audits and assessments", "2": "Enhanced access control measu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1605:
RiskId: 937
ComplianceId: 956
RiskTitle: Surveillance Monitoring Risk
Criticality: Medium
PossibleDamage: Failure to detect security breaches or incidents captured on camera
Category: Operational
RiskType: Residual
BusinessImpact: Increased risk of security incidents going undetected and potential operational disrup
RiskDescription: Inadequate monitoring of surveillance cameras can result in missed security incidents
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regular camera checks and maintenance", "2": "Continuous training for security p
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1606:
RiskId: 938
ComplianceId: 957
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive areas or data
Category: Operational
RiskType: Current
BusinessImpact: Security breaches, data loss, compliance violations
RiskDescription: Unauthorized access to restricted areas or data due to lack of proper visitor access re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access control measures", "2": "Regular audits of access records", "3"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1607:
RiskId: 939
ComplianceId: 958
RiskTitle: Outdated Access Authorizations Risk
Criticality: Medium
PossibleDamage: Outdated access authorizations leading to potential security risks

Category: Operational
RiskType: Current
BusinessImpact: Security breaches, unauthorized access
RiskDescription: Failure to review visitor access records could result in outdated access authorizations
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated anomaly detection tools", "2": "Regular training for security personnel
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1608:
RiskId: 940
ComplianceId: 959
RiskTitle: System Downtime due to Power Equipment Failure
Criticality: High
PossibleDamage: System downtime, data loss, and financial losses
Category: Operational
RiskType: Current
BusinessImpact: Significant disruption to operations and potential loss of revenue
RiskDescription: Failure to protect power equipment could result in unexpected system downtime, lead
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implementing redundant power sources", "2": "Regular testing and maintenance o
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1609:
RiskId: 941
ComplianceId: 960
RiskTitle: Unauthorized Activation of Emergency Shutoff
Criticality: High
PossibleDamage: Data loss, equipment damage, operational disruption
Category: Operational
RiskType: Inherent
BusinessImpact: Facilities management, IT operations
RiskDescription: Unauthorized activation of emergency shutoff switches can lead to sudden power loss
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls for emergency shutoff switches", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1610:
RiskId: 942
ComplianceId: 961
RiskTitle: Delay in Accessing Emergency Shutoff Switches
Criticality: Medium
PossibleDamage: Inability to quickly respond to emergencies, potential damage to critical resources
Category: Operational
RiskType: Inherent
BusinessImpact: Facilities management, IT operations
RiskDescription: If emergency shutoff switches are not easily accessible or their location is not clearly

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update emergency shutoff switch locations", "2": "Provide tr
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1611:
RiskId: 943
ComplianceId: 962
RiskTitle: Power Failure Risk
Criticality: High
PossibleDamage: Data loss, system downtime, and potential injuries
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations and potential financial losses
RiskDescription: Failure to provide emergency power could lead to system shutdowns, data loss, and c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and maintenance of UPS systems", "2": "Training employees on e
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1612:
RiskId: 944

ComplianceId: 963
RiskTitle: Inadequate Emergency Lighting
Criticality: High
PossibleDamage: Risk of accidents, injuries, or delays in evacuation
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, potential injuries to employees or visitors
RiskDescription: Failure of automatic emergency lighting system to activate during power outage or dis
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and maintenance of emergency lighting systems", "2": "Backup po
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1613:
RiskId: 945
ComplianceId: 964
RiskTitle: Contingency Plan Misalignment
Criticality: Medium
PossibleDamage: Risk of inadequate emergency response and recovery
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, potential delays in recovery
RiskDescription: Lack of integration of emergency lighting requirements into the organization's continge
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update of contingency plans", "2": "Integration of emergency
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1614:
RiskId: 946
ComplianceId: 965
RiskTitle: Failure of Fire Detection and Suppression Systems
Criticality: High
PossibleDamage: Extensive damage to facilities, data loss, and potential harm to personnel
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, and reputational damage
RiskDescription: Inadequate fire protection measures may lead to uncontrolled fire outbreaks and seve
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular maintenance and testing of fire detection and suppression systems", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1615:
RiskId: 947
ComplianceId: 966
RiskTitle: Delayed Fire Detection
Criticality: High
PossibleDamage: Extensive property damage and potential loss of life

Category: Operational
RiskType: Inherent
BusinessImpact: Significant financial losses and harm to personnel
RiskDescription: Failure to activate fire detection systems automatically could result in delayed detectio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and maintenance of fire detection systems", "2": "Training personn
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1616:
RiskId: 948
ComplianceId: 967
RiskTitle: Delayed Notification of Emergency Responders
Criticality: Medium
PossibleDamage: Delays in response and increased risk to personnel and property
Category: Operational
RiskType: Inherent
BusinessImpact: Increased harm to personnel and property
RiskDescription: Failure to notify emergency responders promptly could result in delays in response, in
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear notification protocols and contact lists", "2": "Regularly update con
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1617:
RiskId: 949
ComplianceId: 968
RiskTitle: Failure to Activate Fire Suppression Systems
Criticality: High
PossibleDamage: Extensive property damage and potential loss of life
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, and reputational damage
RiskDescription: If fire suppression systems fail to activate during a fire emergency, the organization m
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and maintenance of fire suppression systems", "2": "Training pers
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1618:
RiskId: 950
ComplianceId: 969
RiskTitle: Lack of Continuous Fire Suppression Capability
Criticality: Medium
PossibleDamage: Uncontrolled fires causing extensive damage
Category: Operational
RiskType: Current
BusinessImpact: Property damage, operational disruptions, and potential safety hazards
RiskDescription: If facilities lack continuous fire suppression capability, uncontrolled fires may cause ex

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing automated fire suppression systems", "2": "Regular maintenance a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1619:
RiskId: 951
ComplianceId: 970
RiskTitle: Environmental Control Failure
Criticality: High
PossibleDamage: System downtime, data loss, disruption of business operations
Category: Environmental
RiskType: Residual
BusinessImpact: Significant impact on business operations and reputation
RiskDescription: Failure to maintain environmental control levels can lead to system overheating, hard
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular maintenance and calibration of environmental control systems", "2": "Imp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1620:
RiskId: 952

ComplianceId: 971
RiskTitle: Water Damage Risk in Data Centers
Criticality: High
PossibleDamage: Water damage leading to system downtime and data loss.
Category: Operational
RiskType: Current
BusinessImpact: Significant financial losses and reputational damage.
RiskDescription: Risk of water leakage in data centers due to ineffective valve systems.
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular inspection and maintenance of valves", "2": "Implementing automated wa
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1621:
RiskId: 953
ComplianceId: 972
RiskTitle: Security Breach Due to Unauthorized System Components
Criticality: High
PossibleDamage: Compromise of sensitive information, loss of data integrity, reputational damage.
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of customer trust, financial losses, legal implications.
RiskDescription: Unauthorized system components entering or exiting the facility could lead to security
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement access control measures at entry and exit points", "2": "Regularly audi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1622:
RiskId: 954
ComplianceId: 973
RiskTitle: Unauthorized Access Due to Undocumented Alternate Work Sites
Criticality: High
PossibleDamage: Unauthorized access to sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches and compromise of confidential information.
RiskDescription: Failure to document alternate work sites may result in employees using unauthorized
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to verify documented alternate work sites", "2": "Training for emplo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1623:
RiskId: 955
ComplianceId: 974
RiskTitle: Data Breaches Due to Ineffective Controls at Alternate Work Sites
Criticality: Medium
PossibleDamage: Data breaches and security incidents

Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data and damage to organizational reputation.
RiskDescription: Ineffective controls at alternate work sites may lead to security vulnerabilities, resultin
RiskLikelihood: 5
RiskImpact: 8
RiskExposureRating: 40
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular testing and evaluation of controls at alternate work sites", "2": "Immediate
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1624:
RiskId: 956
ComplianceId: 975
RiskTitle: Non-Compliance with Planning Policy
Criticality: High
PossibleDamage: Legal penalties, security breaches, operational disruptions
Category: Compliance
RiskType: Residual
BusinessImpact: Legal and operational consequences affecting all business units
RiskDescription: Failure to comply with planning policy may result in legal violations, security breaches
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular legal and regulatory compliance reviews", "2": "Training programs for per
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1625:
RiskId: 957
ComplianceId: 976
RiskTitle: Lack of Designated Planning Policy Official
Criticality: Medium
PossibleDamage: Confusion, delays, inconsistencies in policy management
Category: Operational
RiskType: Residual
BusinessImpact: Operational efficiency and policy adherence compromised
RiskDescription: Absence of a designated official for planning policy management may result in confus
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clearly defined roles and responsibilities for the designated official", "2": "Regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1626:
RiskId: 958
ComplianceId: 977
RiskTitle: Outdated Planning Policy and Procedures
Criticality: Medium
PossibleDamage: Non-compliance, security vulnerabilities, inefficiencies
Category: IT
RiskType: Residual
BusinessImpact: IT systems and processes affected by outdated policies and procedures
RiskDescription: Failure to review and update planning policy and procedures may result in non-compl

RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular policy and procedure reviews", "2": "Automated alerts for update requirem
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1627:
RiskId: 959
ComplianceId: 978
RiskTitle: Misalignment of Security and Privacy Plans with Enterprise Architecture
Criticality: High
PossibleDamage: Ineffective controls and increased risk exposure
Category: Operational
RiskType: Current
BusinessImpact: Potential security breaches or privacy violations
RiskDescription: Failure to align security and privacy plans with enterprise architecture may result in ga
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Engage enterprise architects in the development of security and privacy plans", "2
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1628:
RiskId: 960

ComplianceId: 979
RiskTitle: Failure to Identify Information Types Processed, Stored, and Transmitted
Criticality: Medium
PossibleDamage: Inadequate protection of sensitive data and increased risk of data breaches
Category: IT
RiskType: Current
BusinessImpact: Potential data breaches or privacy violations
RiskDescription: Failure to identify information types processed, stored, and transmitted by the system
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Conduct data classification exercises to identify information types", "2": "Impleme
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1629:
RiskId: 961
ComplianceId: 980
RiskTitle: Unauthorized Access and Data Breach Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, reputational damage, legal consequences
RiskDescription: The risk of unauthorized access and data breaches due to non-compliance with rules
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for access control", "2": "Regularly review a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1630:
RiskId: 962
ComplianceId: 981
RiskTitle: Lack of Documented Acknowledgment Risk
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information, data breaches, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, reputational damage, legal consequences
RiskDescription: The risk of unauthorized access and data breaches due to lack of documented ackno
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated acknowledgment systems for access control", "2": "Regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1631:
RiskId: 963
ComplianceId: 982
RiskTitle: Unauthorized Access to Organizational Information
Criticality: High
PossibleDamage: Data breaches, exposure of personally identifiable information

Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of customer trust and legal consequences
RiskDescription: Unauthorized entities gaining access to non-public organizational information through
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on social media policies and best practices", "2": "Implementation
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1632:
RiskId: 964
ComplianceId: 983
RiskTitle: Unauthorized Disclosure of Organizational Information
Criticality: Medium
PossibleDamage: Competitive disadvantage, loss of intellectual property
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of market share and revenue
RiskDescription: Organizational information being posted on public websites by personnel
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Training on data protection and confidentiality policies", "2": "Implementation of ap
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1633:
RiskId: 965
ComplianceId: 984
RiskTitle: Failure to Develop Security and Privacy Architectures
Criticality: High
PossibleDamage: Unauthorized access, data breaches, privacy violations, regulatory fines
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units may suffer financial, reputational, and legal consequences
RiskDescription: Failure to develop security and privacy architectures may result in unauthorized acces
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update security and privacy architectures", "2": "Integrate ar
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1634:
RiskId: 966
ComplianceId: 985
RiskTitle: Failure to Review and Update Security and Privacy Architectures
Criticality: Medium
PossibleDamage: Outdated security measures, vulnerabilities, non-compliance with regulations
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face increased security risks and potential non-compliance iss
RiskDescription: Failure to review and update security and privacy architectures may result in outdated

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a regular review schedule for architectures", "2": "Document changes in
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1635:
RiskId: 967
ComplianceId: 986
RiskTitle: Failure to Reflect Planned Architecture Changes in Security and Privacy Plans
Criticality: High
PossibleDamage: Misalignment between security measures and system architecture, security vulnerab
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face increased security risks and operational inefficiencies
RiskDescription: Failure to reflect planned architecture changes in security and privacy plans may resu
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update security and privacy plans with architecture changes", "2": "Com
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1636:
RiskId: 968

ComplianceId: 987
RiskTitle: Inadequate Protection due to Incorrect Control Baseline Selection
Criticality: High
PossibleDamage: Data breaches, compliance violations, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, legal consequences, and damage to reputation
RiskDescription: Failure to select an appropriate control baseline may result in inadequate protection o
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct a thorough review of stakeholder needs and applicable mandates", "2": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1637:
RiskId: 969
ComplianceId: 988
RiskTitle: Inadequate Control Baseline Tailoring
Criticality: High
PossibleDamage: Potential data breaches or non-compliance penalties
Category: Operational
RiskType: Residual
BusinessImpact: All business units may face financial losses and reputational damage.
RiskDescription: Failure to tailor control baselines may result in inadequate protection against threats a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular review and update of tailored control baselines", "2": "Continuous monito
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1638:
RiskId: 970
ComplianceId: 989
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of sensitive data, compromised security measures
RiskDescription: Unauthorized access to critical systems and data due to lack of clear personnel secur
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and authentication measures", "2": "Regular secu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1639:
RiskId: 971
ComplianceId: 990
RiskTitle: Policy Oversight Risk
Criticality: Medium
PossibleDamage: Inconsistent policy management, lack of oversight in personnel security controls

Category: Operational
RiskType: Current
BusinessImpact: Potential gaps in policy implementation and enforcement
RiskDescription: Lack of designated official may lead to inconsistent policy management and oversight
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear role definition and responsibilities for the designated official", "2": "Regular r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1640:
RiskId: 972
ComplianceId: 991
RiskTitle: Outdated Policy Risk
Criticality: High
PossibleDamage: Non-compliance with updated regulations, security incidents due to outdated policies
Category: Operational
RiskType: Current
BusinessImpact: Potential security incidents and breaches
RiskDescription: Outdated policy and procedures may not align with current security requirements and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reviews and updates based on changes in regulations and security lands
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1641:
RiskId: 973
ComplianceId: 992
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Potential breach of national security and organizational integrity.
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of sensitive information, reputational damage, legal implications.
RiskDescription: Unauthorized individuals gaining access to sensitive information due to improperly as
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls based on risk designations", "2": "Regularly revie
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1642:
RiskId: 974
ComplianceId: 993
RiskTitle: Unsuitable Individuals in Positions
Criticality: Medium
PossibleDamage: Decreased operational efficiency and potential security risks.
Category: Operational
RiskType: Inherent
BusinessImpact: Inefficient operations, potential security breaches.
RiskDescription: Individuals not suited for the risk level of their positions due to lack of screening criteri

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear screening criteria based on risk designations", "2": "Provide trainin
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1643:
RiskId: 975
ComplianceId: 994
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breach resulting in financial loss and reputational damage.
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust and legal implications.
RiskDescription: Unauthorized access to sensitive information can lead to data breaches, financial loss
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access control", "2": "Regularly audit access logs", "3": "En
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1644:
RiskId: 976

ComplianceId: 995
RiskTitle: Outdated Background Check Risk
Criticality: Medium
PossibleDamage: Compromised data security and regulatory non-compliance.
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions and potential legal consequences.
RiskDescription: Failure to rescreen individuals can lead to compromised data security, operational dis
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated rescreening reminders", "2": "Conduct periodic security awa
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1645:
RiskId: 977
ComplianceId: 996
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, leaks, misuse of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, reputational damage, regulatory fines
RiskDescription: Unauthorized individuals gaining access to controlled unclassified information due to
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for access control", "2": "Regularly review a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1646:
RiskId: 978
ComplianceId: 997
RiskTitle: Unauthorized System Access by Terminated Individuals
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, and potential harm to
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential data breaches and reputational dam
RiskDescription: Terminated individuals retaining system access could lead to unauthorized data acces
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated system access disabling procedures", "2": "Regularly revie
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1647:
RiskId: 979
ComplianceId: 998
RiskTitle: Lack of Awareness of Security Constraints by Terminated Individuals
Criticality: Medium
PossibleDamage: Lack of awareness of security constraints, potential breaches of confidentiality, and

Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential breaches of confidentiality and lega
RiskDescription: Terminated individuals not understanding security constraints could lead to breaches
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide comprehensive training on security policies and procedures", "2": "Docum
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1648:
RiskId: 980
ComplianceId: 999
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, security incidents, and compliance violations.
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, reputation damage, and financial losses.
RiskDescription: Unauthorized access to systems and facilities due to misaligned access authorization
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews and audits", "2": "Implementing role-based access contro
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1649:
RiskId: 981
ComplianceId: 1000
RiskTitle: Transfer Actions Delay Risk
Criticality: Medium
PossibleDamage: Operational disruptions, delays in access provisioning, and security vulnerabilities.
Category: Operational
RiskType: Residual
BusinessImpact: Operational delays, security vulnerabilities, and potential compliance issues.
RiskDescription: Delays in initiating transfer actions can lead to operational disruptions, delays in acces
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear transfer protocols and timelines", "2": "Automate transfer processe
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1650:
RiskId: 982
ComplianceId: 1001
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, breach of confidentiality, legal implicat
Category: Compliance
RiskType: Residual
BusinessImpact: All business units would be impacted by unauthorized access
RiskDescription: Risk of unauthorized access to organizational systems leading to potential data breac

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication measures", "2": "Regular access reviews and au
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1651:
RiskId: 983
ComplianceId: 1002
RiskTitle: Outdated Agreements Risk
Criticality: Medium
PossibleDamage: Outdated agreements leading to non-compliance, increased risk of unauthorized acc
Category: Compliance
RiskType: Residual
BusinessImpact: All business units would be impacted by non-compliance
RiskDescription: Risk of using outdated access agreements leading to non-compliance with organizatio
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated agreement review processes", "2": "Regular communication on update
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1652:
RiskId: 984

ComplianceId: 1005
RiskTitle: Inconsistent Enforcement of Sanctions
Criticality: High
PossibleDamage: Data breaches, legal liabilities, and reputational harm
Category: Compliance
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to enforce sanctions may result in repeated non-compliance, increased securi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on policies and procedures", "2": "Clear communication of conse
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1653:
RiskId: 985
ComplianceId: 1006
RiskTitle: Delayed Notification of Employee Sanctions
Criticality: Medium
PossibleDamage: Confusion, lack of accountability, and legal challenges
Category: Compliance
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to notify organization-defined personnel or roles within organization-defined ti
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear notification procedures", "2": "Automate notification process where

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1654:

RiskId: 986

ComplianceId: 1007

RiskTitle: Role Ambiguity and Increased Risk of Data Breaches

Criticality: High

PossibleDamage: Data breaches, loss of sensitive information, regulatory fines

Category: Operational

RiskType: Inherent

BusinessImpact: Potential disruption to operations, financial losses, damage to reputation

RiskDescription: Failure to clearly define security and privacy roles in position descriptions may lead to

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular review and update of position descriptions to align with current security a

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1655:

RiskId: 987

ComplianceId: 1008

RiskTitle: Inadequate risk assessment policy

Criticality: High

PossibleDamage: Increased vulnerability to security breaches, legal consequences, and regulatory fine

Category: Compliance
RiskType: Current
BusinessImpact: All business units may face operational disruptions, financial losses, and reputational
RiskDescription: Failure to have a comprehensive risk assessment policy may expose the organization
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on risk assessment policy", "2": "Period
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1656:
RiskId: 988
ComplianceId: 1009
RiskTitle: Lack of designated official for risk assessment policy
Criticality: Medium
PossibleDamage: Confusion, delays, and inconsistencies in policy management
Category: Operational
RiskType: Current
BusinessImpact: Operational inefficiencies, delays in policy implementation, and potential compliance
RiskDescription: Not having a designated official for managing risk assessment policy may result in un
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear delineation of roles and responsibilities of the designated official", "2": "Reg
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1657:
RiskId: 989
ComplianceId: 1010
RiskTitle: Outdated risk assessment policy and procedures
Criticality: High
PossibleDamage: Ineffective risk management, increased vulnerabilities, and non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, security incidents, and legal consequences
RiskDescription: Failure to review and update risk assessment policy and procedures may result in out
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy and procedure reviews based on industry best practices", "2": "Tim
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1658:
RiskId: 990
ComplianceId: 1011
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information and compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, reputational damage, legal consequences
RiskDescription: Unauthorized access to sensitive information due to inaccurate system categorization

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls", "2": "Regular security audits", "3": "Encryption
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1659:
RiskId: 991
ComplianceId: 1012
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Potential exposure of sensitive information and harm to individuals' personally identi
Category: Operational
RiskType: Inherent
BusinessImpact: Significant impact on operations and reputation
RiskDescription: Failure to conduct proper risk assessments may lead to data breaches and unauthoriz
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on risk assessment procedures", "2": "Implementing automated r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1660:
RiskId: 992

ComplianceId: 1013
RiskTitle: Supply Chain Risk Exposure
Criticality: High
PossibleDamage: Failure to mitigate supply chain risks may lead to significant impact on organizationa
Category: Operational
RiskType: Current
BusinessImpact: All business units within the organization
RiskDescription: Failure to assess and mitigate supply chain risks could result in supply chain-related e
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular supply chain risk assessments", "2": "Implementing supply chain risk miti
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1661:
RiskId: 993
ComplianceId: 1016
RiskTitle: Exploitation of Unpatched Vulnerabilities
Criticality: High
PossibleDamage: Data breaches, system compromise, financial loss, reputational damage
Category: IT
RiskType: Current
BusinessImpact: Potential compromise of critical systems and sensitive data
RiskDescription: Failure to update vulnerabilities may result in malicious actors exploiting known vulne
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly update vulnerabilities for scanning", "2": "Implement network segmenta
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1662:
RiskId: 994
ComplianceId: 1017
RiskTitle: Undetected Vulnerabilities
Criticality: High
PossibleDamage: System compromise, data breaches, financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, damage to reputation, legal implications
RiskDescription: Failure to define vulnerability scanning coverage may result in undetected vulnerabilit
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of vulnerability scanning coverage definitions", "2": "P
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1663:
RiskId: 995
ComplianceId: 1018
RiskTitle: Limited Vulnerability Coverage
Criticality: Medium
PossibleDamage: Increased risk of security incidents

Category: IT
RiskType: Inherent
BusinessImpact: Increased likelihood of security breaches, data loss, and system compromise
RiskDescription: Relying on a single scanning tool may result in limited coverage and missed vulnerab
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular assessment and integration of new scanning tools", "2": "Continuous mor
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1664:
RiskId: 996
ComplianceId: 1019
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: IT, Security
RiskDescription: Unauthorized access to classified or controlled unclassified information can lead to da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement privileged access controls", "2": "Regularly audit access logs", "3": "Pr
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1665:
RiskId: 997
ComplianceId: 1020
RiskTitle: Unauthorized Access and System Downtime
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, system downtime, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of data confidentiality, system availability, and reputation
RiskDescription: Failure to establish a public reporting channel may result in unidentified vulnerabilities
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust access controls and monitoring mechanisms", "2": "Regularly u
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1666:
RiskId: 998
ComplianceId: 1021
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of sensitive data, regulatory fines, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: All business units may experience financial and reputational losses
RiskDescription: Risk of unauthorized access to sensitive data due to inadequate response to security

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption measures", "2": "Enhance access controls", "3": "Conduct r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1667:
RiskId: 999
ComplianceId: 1022
RiskTitle: Inadequate Protection of Critical System Components and Functions
Criticality: High
PossibleDamage: Potential system failures or security breaches due to inadequate protection measure
Category: Operational
RiskType: Inherent
BusinessImpact: Systems Engineering, Information Security, and Development projects may be disrup
RiskDescription: Failure to identify critical system components and functions through criticality analysis
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Perform regular audits to ensure criticality analysis is conducted at designated de
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1668:
RiskId: 1000

ComplianceId: 1023
RiskTitle: Inadequate system and services acquisition policy
Criticality: High
PossibleDamage: Non-compliance with policy may lead to legal consequences, security breaches, and
Category: Operational
RiskType: Current
BusinessImpact: Potential legal fines, loss of sensitive data, and disruption of operations
RiskDescription: Failure to comply with policy requirements may result in inadequate controls, increase
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Training programs for policy implemen
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1669:
RiskId: 1001
ComplianceId: 1024
RiskTitle: Lack of designated official for policy management
Criticality: Medium
PossibleDamage: Inconsistent policy implementation, gaps in policy coverage, and increased risk expo
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, potential compliance issues, and increased vulnerability to ris
RiskDescription: Absence of a designated official may result in unclear responsibilities, lack of oversigh
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Clear definition of official roles", "2": "Regular performance evaluations", "3": "Bac
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1670:
RiskId: 1002
ComplianceId: 1025
RiskTitle: Outdated system and services acquisition policy and procedures
Criticality: High
PossibleDamage: Non-compliance, security incidents, and operational disruptions due to ineffective co
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, potential legal consequences, and compromised security pos
RiskDescription: Failure to review and update policies and procedures may result in ineffective control
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear review schedules", "2": "Regular training on updates", "3": "Autom
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1671:
RiskId: 1003
ComplianceId: 1026
RiskTitle: Inadequate Protection of Sensitive Data
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Loss of customer trust, financial penalties, legal consequences
RiskDescription: Failure to identify high-level security and privacy requirements may result in inadequa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct thorough risk assessment workshops with key stakeholders", "2": "Engag
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1672:
RiskId: 1004
ComplianceId: 1027
RiskTitle: Underfunded Security Measures
Criticality: Medium
PossibleDamage: Vulnerability to cyber threats, compliance violations
Category: Financial
RiskType: Inherent
BusinessImpact: Financial losses, regulatory penalties
RiskDescription: Failure to allocate adequate resources for security and privacy measures may result i
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and adjust budget allocations based on security risk assessmen
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1673:
RiskId: 1005
ComplianceId: 1028
RiskTitle: Security and Privacy Vulnerabilities in System Development Life Cycle
Criticality: High
PossibleDamage: Security breaches, data leaks, privacy violations
Category: Operational
RiskType: Residual
BusinessImpact: IT, Security, Privacy departments
RiskDescription: Failure to incorporate security and privacy considerations in the system development
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security and privacy audits during system development", "2": "Ongoing tr
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1674:
RiskId: 1006
ComplianceId: 1029
RiskTitle: Unclear Information Security and Privacy Roles and Responsibilities
Criticality: Medium
PossibleDamage: Security gaps, privacy violations
Category: Operational
RiskType: Residual
BusinessImpact: IT, Security, Privacy departments
RiskDescription: Lack of clarity in information security and privacy roles and responsibilities may result

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update role definitions and responsibilities", "2": "Provide tra
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1675:
RiskId: 1007
ComplianceId: 1030
RiskTitle: Unmanaged Information Security and Privacy Risks in System Development Life Cycle
Criticality: High
PossibleDamage: Security incidents, privacy breaches
Category: Operational
RiskType: Residual
BusinessImpact: IT, Security, Privacy departments
RiskDescription: Failure to integrate risk management into system development life cycle activities may
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular risk assessments during system development", "2": "Implement risk treat
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1676:
RiskId: 1008

ComplianceId: 1031
RiskTitle: Inadequate Security and Privacy Functional Requirements in Acquisition Contract
Criticality: High
PossibleDamage: Data breaches, unauthorized access, and non-compliance with regulations
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units involved in the acquisition process may be impacted by security inc
RiskDescription: Failure to include security and privacy functional requirements in the acquisition contr
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure thorough review of the acquisition contract by legal and compliance teams
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1677:
RiskId: 1009
ComplianceId: 1032
RiskTitle: Unauthorized Access to Security and Privacy Documentation
Criticality: Medium
PossibleDamage: Security breaches, data leaks, and non-compliance with regulations
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units involved in the acquisition process may be impacted by security inc
RiskDescription: Unauthorized access to security and privacy documentation may lead to security brea
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement access controls and encryption for sensitive documentation", "2": "Reg
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1678:
RiskId: 1010
ComplianceId: 1033
RiskTitle: Undefined Acceptance Criteria in Acquisition Contracts
Criticality: High
PossibleDamage: Vulnerabilities, non-compliance, and security incidents
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units involved in the acquisition process may be impacted by security inc
RiskDescription: Undefined acceptance criteria may result in the acquisition of systems that do not me
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Involve security experts in defining acceptance criteria", "2": "Conduct thorough te
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1679:
RiskId: 1011
ComplianceId: 1034
RiskTitle: Unauthorized Access through Undocumented Interfaces
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, data breaches, system compromise

Category: IT
RiskType: Current
BusinessImpact: IT, Security, Compliance
RiskDescription: Failure to document security-relevant external system interfaces may lead to unautho
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of external system interfaces documentation", "2": "Training develo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1680:
RiskId: 1012
ComplianceId: 1035
RiskTitle: Inefficient Control Implementation due to Lack of High-Level Design
Criticality: Medium
PossibleDamage: Inefficient control implementation, system vulnerabilities
Category: IT
RiskType: Current
BusinessImpact: IT, Security, Compliance
RiskDescription: Failure to document high-level design may lead to inefficiencies in control implementa
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular reviews of high-level design documentation", "2": "Engaging stakeholders
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1681:
RiskId: 1013
ComplianceId: 1036
RiskTitle: Security Vulnerabilities Due to Unidentified Functions, Ports, Protocols, and Services
Criticality: High
PossibleDamage: Potential security breaches, data leaks, system downtime
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive data, reputational damage, financial losses
RiskDescription: Failure to identify and control functions, ports, protocols, and services may expose the
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement network segmentation", "2": "Enforce strict access controls", "3": "Regu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1682:
RiskId: 1014
ComplianceId: 1037
RiskTitle: Non-Compliant Product Usage Risk
Criticality: High
PossibleDamage: Unauthorized access and data breaches
Category: IT
RiskType: Residual
BusinessImpact: IT, Security
RiskDescription: The risk of using non-approved products for PIV capability leading to vulnerabilities ar

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure only approved products are in use", "2": "Strict enforcem
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1683:
RiskId: 1015
ComplianceId: 1038
RiskTitle: Outdated Product Risk
Criticality: Medium
PossibleDamage: Security vulnerabilities due to outdated products
Category: IT
RiskType: Residual
BusinessImpact: IT, Security
RiskDescription: The risk of using outdated products for PIV capability that may not meet current secur
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly check NIST updates for approved products", "2": "Establish a process f
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1684:
RiskId: 1016

ComplianceId: 1039
RiskTitle: Inadequate Administrator Documentation
Criticality: High
PossibleDamage: Misconfigurations, security vulnerabilities, unauthorized access
Category: IT
RiskType: Current
BusinessImpact: Disruption of IT operations, potential data breaches
RiskDescription: Lack of proper administrator documentation can lead to misconfigurations, security vu
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for system administrators on secure configuration practices", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1685:
RiskId: 1017
ComplianceId: 1040
RiskTitle: Inadequate User Documentation
Criticality: Medium
PossibleDamage: Insecure system usage, data breaches, privacy violations
Category: IT
RiskType: Current
BusinessImpact: Data breaches, privacy violations
RiskDescription: Insufficient user documentation can lead to insecure system usage, unauthorized acc
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "User training on security best practices and system usage guidelines", "2": "Regu

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1686:

RiskId: 1018

ComplianceId: 1041

RiskTitle: Lack of System Documentation

Criticality: High

PossibleDamage: Hindered system understanding, increased security risks, impacted incident respons

Category: IT

RiskType: Current

BusinessImpact: Security vulnerabilities, supply chain disruptions

RiskDescription: Absence of system documentation can lead to difficulties in system understanding, he

RiskLikelihood: 8

RiskImpact: 8

RiskExposureRating: 64

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear documentation retrieval procedures", "2": "Engage with manufactu

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1687:

RiskId: 1019

ComplianceId: 1042

RiskTitle: Data Breach Risk

Criticality: High

PossibleDamage: Loss of sensitive data, legal liabilities, reputational damage

Category: IT
RiskType: Residual
BusinessImpact: Financial loss, legal consequences, damage to reputation
RiskDescription: Unauthorized access to sensitive data due to inadequate security measures
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implementing multi-factor authentication", "2": "Regularly monitoring and analyzin
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1688:
RiskId: 1020
ComplianceId: 1043
RiskTitle: Software Vulnerability Risk
Criticality: Medium
PossibleDamage: Exploitation of software vulnerabilities, data breaches, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Financial loss, legal consequences, damage to reputation
RiskDescription: Introduction of security vulnerabilities in software code due to lack of developer trainin
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing secure coding guidelines", "2": "Conducting regular security training
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1689:
RiskId: 1021
ComplianceId: 1044
RiskTitle: Non-Compliance by External Service Providers
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, breaches of privacy regulations
Category: Operational
RiskType: Current
BusinessImpact: All business units utilizing external system services
RiskDescription: Failure of external service providers to comply with security and privacy requirements
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of provider compliance", "2": "Implement strong contractual agreer
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1690:
RiskId: 1022
ComplianceId: 1045
RiskTitle: Undefined Organizational Oversight and User Roles
Criticality: Medium
PossibleDamage: Confusion, mismanagement, or misuse of external system services
Category: Operational
RiskType: Current
BusinessImpact: All business units utilizing external system services
RiskDescription: Lack of defined roles and responsibilities for oversight and usage of external system s

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on roles and responsibilities", "2": "Clear documentation of user r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1691:
RiskId: 1023
ComplianceId: 1046
RiskTitle: Lack of Monitoring Control Compliance by External Service Providers
Criticality: High
PossibleDamage: Undetected non-compliance issues, security breaches
Category: Operational
RiskType: Current
BusinessImpact: All business units utilizing external system services
RiskDescription: Failure to monitor control compliance by external service providers may result in unde
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits and assessments of provider compliance", "2": "Automated monito
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1692:
RiskId: 1024

ComplianceId: 1047
RiskTitle: Inadequate Information Security Services Acquisition
Criticality: High
PossibleDamage: Potential security breaches, data loss, and compromised systems.
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, financial losses, damage to reputation.
RiskDescription: Failure to conduct a risk assessment prior to acquiring information security services m
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Engage a qualified risk assessment team to conduct a thorough analysis", "2": "In
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1693:
RiskId: 1025
ComplianceId: 1048
RiskTitle: Unauthorized Outsourcing of Information Security Services
Criticality: Medium
PossibleDamage: Non-compliance with regulations, security vulnerabilities, legal disputes.
Category: Legal
RiskType: Inherent
BusinessImpact: Legal penalties, financial losses, damage to reputation.
RiskDescription: Failure to obtain proper approvals for outsourcing information security services may re
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish clear approval processes and documentation requirements", "2": "Imple
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1694:
RiskId: 1026
ComplianceId: 1049
RiskTitle: Failure to Identify External System Services Functions
Criticality: Medium
PossibleDamage: Incompatible services, security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: Disruption of services, potential data breaches
RiskDescription: Failure to identify the required functions for external system services may lead to com
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular audits of identified functions", "2": "Training for staff on function identifica
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1695:
RiskId: 1027
ComplianceId: 1050
RiskTitle: Failure to Identify External System Services Ports and Protocols
Criticality: High
PossibleDamage: Network incompatibility, security vulnerabilities

Category: IT
RiskType: Current
BusinessImpact: Network disruptions, potential security breaches
RiskDescription: Failure to identify the required ports and protocols for external system services may le
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of identified ports and protocols", "2": "Documentation of network c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1696:
RiskId: 1028
ComplianceId: 1051
RiskTitle: Risk of Unauthorized Access and Data Breaches
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Disruption of business operations, loss of customer trust
RiskDescription: Unauthorized access to sensitive information or data breaches due to lack of control o
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls and encryption measures", "2": "Regularly mon
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1697:
RiskId: 1029
ComplianceId: 1052
RiskTitle: Risk of Data Breaches and Regulatory Non-Compliance
Criticality: Medium
PossibleDamage: Financial penalties, reputational harm, data loss
Category: IT
RiskType: Current
BusinessImpact: Disruption of data management operations, regulatory scrutiny
RiskDescription: Data breaches or regulatory non-compliance due to lack of control over data storage l
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement data encryption and access controls", "2": "Regularly review and upda
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1698:
RiskId: 1030
ComplianceId: 1053
RiskTitle: Unauthorized Changes to Configuration Items
Criticality: High
PossibleDamage: System vulnerabilities, security breaches, and unauthorized access
Category: Operational
RiskType: Current
BusinessImpact: Impact on system integrity, data confidentiality, and availability
RiskDescription: Unauthorized changes to configuration items could compromise the security and integ

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls to configuration items", "2": "Regularly review an
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1699:
RiskId: 1031
ComplianceId: 1054
RiskTitle: Implementation of Unauthorized Changes
Criticality: Medium
PossibleDamage: System instability, vulnerabilities, or functionality issues
Category: Operational
RiskType: Current
BusinessImpact: Impact on system functionality, reliability, and security
RiskDescription: Implementation of unauthorized changes could lead to system instability, vulnerabilitie
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement change control processes", "2": "Require approval for all changes befo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1700:
RiskId: 1032

ComplianceId: 1055
RiskTitle: Unidentified Security Vulnerabilities and Privacy Risks
Criticality: High
PossibleDamage: Data breaches, unauthorized access, non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Development delays, reputational damage, legal consequences
RiskDescription: Failure to conduct ongoing security and privacy control assessments may result in un
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for developers on security and privacy
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1701:
RiskId: 1033
ComplianceId: 1056
RiskTitle: Inadequate System Testing
Criticality: Medium
PossibleDamage: System vulnerabilities, data breaches, non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Data breaches, system downtime, reputational damage
RiskDescription: Insufficient system testing may result in undetected vulnerabilities, leading to potentia
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement automated testing tools to increase test coverage and efficiency", "2":

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1702:

RiskId: 1034

ComplianceId: 1057

RiskTitle: Undetected Vulnerabilities in Code

Criticality: High

PossibleDamage: Potential security breaches

Category: IT

RiskType: Current

BusinessImpact: Development delays, compromised customer data

RiskDescription: Failure to detect vulnerabilities in the code can lead to exploitation by malicious actors

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on secure coding practices", "2": "Implementing code review proc

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 1703:

RiskId: 1035

ComplianceId: 1058

RiskTitle: Undetected Vulnerabilities

Criticality: High

PossibleDamage: System compromises, data breaches, financial losses

Category: IT
RiskType: Residual
BusinessImpact: Development delays, reputation damage, financial losses
RiskDescription: Failure to detect vulnerabilities may expose the system to exploitation by malicious ac
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security training for developers", "2": "Automated vulnerability scanning t
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1704:
RiskId: 1036
ComplianceId: 1059
RiskTitle: Lack of Documentation Risk
Criticality: Medium
PossibleDamage: Misunderstandings, errors, security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: Development delays, reputation damage, financial losses
RiskDescription: Failure to document the development process may result in unclear requirements, inc
RiskLikelihood: 8
RiskImpact: 7
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on documentation best practices", "2": "Documentation review by
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1705:
RiskId: 1037
ComplianceId: 1060
RiskTitle: Unauthorized Changes Risk
Criticality: High
PossibleDamage: Vulnerabilities, compromised system integrity, supply chain risks
Category: IT
RiskType: Current
BusinessImpact: System downtime, data breaches, financial losses
RiskDescription: Unauthorized changes to tools and processes can introduce vulnerabilities, comprom
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls for tool configurations", "2": "Regular audits of tool and
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 1706:
RiskId: 1038
ComplianceId: 1061
RiskTitle: Inaccurate Criticality Assessments
Criticality: High
PossibleDamage: Failure to comply may result in inadequate security measures for high value assets
Category: Operational
RiskType: Current
BusinessImpact: Development delays, security vulnerabilities, potential data breaches
RiskDescription: Failure to conduct criticality analysis by developers may lead to inaccurate assessme

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training to developers on criticality analysis techniques", "2": "Implement a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1707:
RiskId: 1039
ComplianceId: 1062
RiskTitle: Security Breach Due to Unsupported Components
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, financial loss, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties, legal consequences
RiskDescription: Failure to replace unsupported components may expose the organization to security b
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly monitor vendor support status for system components", "2": "Establish a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1708:
RiskId: 1040

ComplianceId: 1063
RiskTitle: System Downtime Due to Lack of Alternative Support
Criticality: Medium
PossibleDamage: Inability to perform critical functions, financial loss, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of productivity, financial penalties, customer dissatisfaction
RiskDescription: Failure to provide alternative support for unsupported components may result in syste
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish contracts with external providers for ongoing support", "2": "Develop cus
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1709:
RiskId: 1041
ComplianceId: 1064
RiskTitle: Inadequate system and communications protection policy
Criticality: High
PossibleDamage: Security breaches, data leaks, service disruptions
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, damage to reputation, legal consequences
RiskDescription: Failure to have a robust policy in place may lead to vulnerabilities in system and comm
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular policy reviews and updates based on emerging threats", "2": "Implementa

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1710:

RiskId: 1042

ComplianceId: 1065

RiskTitle: Inadequate oversight of system and communications protection policy

Criticality: Medium

PossibleDamage: Inconsistent policy implementation, mismanagement of policy

Category: Operational

RiskType: Residual

BusinessImpact: Operational disruptions, security vulnerabilities, compliance issues

RiskDescription: Lack of designated official may lead to gaps in policy oversight and implementation.

RiskLikelihood: 5

RiskImpact: 7

RiskExposureRating: 35

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regular audits and reviews of policy implementation", "2": "Training and support f

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 1711:

RiskId: 1043

ComplianceId: 1066

RiskTitle: Outdated system and communications protection policy

Criticality: High

PossibleDamage: Security incidents, data breaches, non-compliance

Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, damage to reputation, legal consequences
RiskDescription: Failure to update policies may result in inadequate protection against evolving threats
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates based on threat intelligence", "2": "Incident re
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1712:
RiskId: 1044
ComplianceId: 1067
RiskTitle: Unauthorized Access to System Management Functions
Criticality: High
PossibleDamage: Data breaches, system downtime, and loss of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Loss of data integrity, system availability, and reputation damage.
RiskDescription: Unauthorized access to system management functions can lead to unauthorized char
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access control for system management functions", "2": "Re
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1713:
RiskId: 1045
ComplianceId: 1068
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, loss of intellectual property, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties, legal consequences
RiskDescription: Unauthorized access to shared system resources can lead to the exposure of sensitiv
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls and encryption on shared system resources", "2": "Re
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1714:
RiskId: 1046
ComplianceId: 1069
RiskTitle: Denial-of-Service Attack Risk
Criticality: High
PossibleDamage: Loss of critical data, downtime, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: IT, Network Security
RiskDescription: Potential for malicious actors to disrupt services or gain unauthorized access

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement DDoS protection services", "2": "Regularly conduct penetration testing
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1715:
RiskId: 1047
ComplianceId: 1070
RiskTitle: Denial-of-Service Control Failure Risk
Criticality: Medium
PossibleDamage: Service disruption, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: IT, Network Security
RiskDescription: Failure to effectively implement controls may lead to service disruptions and financial
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update control measures", "2": "Conduct regular security as
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1716:
RiskId: 1048

ComplianceId: 1071
RiskTitle: Unauthorized Access at Managed Interfaces
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, network compromise
Category: IT
RiskType: Residual
BusinessImpact: IT, Security
RiskDescription: Unauthorized access at managed interfaces can lead to data breaches, network comp
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement intrusion detection and prevention systems", "2": "Regularly update fire
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1717:
RiskId: 1049
ComplianceId: 1072
RiskTitle: Unauthorized Access to Publicly Accessible Components
Criticality: Medium
PossibleDamage: Unauthorized access to publicly accessible components, data breaches
Category: IT
RiskType: Residual
BusinessImpact: IT, Security
RiskDescription: Unauthorized access to publicly accessible components can lead to data breaches ar
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement network segmentation", "2": "Implement access control lists", "3": "Reg
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1718:
RiskId: 1050
ComplianceId: 1073
RiskTitle: Unauthorized Access to External Networks
Criticality: High
PossibleDamage: Unauthorized access to external networks, data breaches, network compromise
Category: IT
RiskType: Residual
BusinessImpact: IT, Security
RiskDescription: Unauthorized access to external networks can lead to data breaches, network compro
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement secure VPN connections", "2": "Regularly update boundary protection
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1719:
RiskId: 1051
ComplianceId: 1074
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, data breaches, and network vulnerabilities

Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, loss of sensitive information, reputational damage
RiskDescription: Unauthorized individuals gaining access to the network can lead to data breaches, los
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication mechanisms", "2": "Regularly update and patch
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1720:
RiskId: 1052
ComplianceId: 1075
RiskTitle: Unauthorized Access to External Telecommunication Services
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, potential data breaches
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Unauthorized access to external telecommunication services can lead to data breach
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls", "2": "Regular security audits", "3": "Employee
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1721:
RiskId: 1053
ComplianceId: 1076
RiskTitle: Unauthorized Data Transfer Across Managed Interfaces
Criticality: Medium
PossibleDamage: Data leakage, unauthorized data transfer
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, reputational damage
RiskDescription: Failure to establish traffic flow policies can lead to unauthorized data transfer and pote
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update of traffic flow policies", "2": "Implementing encryption f
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1722:
RiskId: 1054
ComplianceId: 1077
RiskTitle: Unauthorized Network Access
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, financial losses
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of customer trust and financial penalties
RiskDescription: Unauthorized network access could lead to data breaches and compromise sensitive

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access control measures", "2": "Regularly monitor network traffi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1723:
RiskId: 1055
ComplianceId: 1078
RiskTitle: Unauthorized Access to Designated Systems
Criticality: Medium
PossibleDamage: Data breaches, loss of sensitive information, system vulnerabilities
Category: IT
RiskType: Residual
BusinessImpact: Potential disruption of critical business operations and loss of sensitive data
RiskDescription: Unauthorized access to designated systems could lead to data breaches and compro
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement strict access control policies for designated systems", "2": "Regularly m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1724:
RiskId: 1056

ComplianceId: 1079
RiskTitle: Unauthorized External Connections and Data Breaches
Criticality: High
PossibleDamage: Unauthorized external connections, data breaches, and loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive information and damage to organizational reputation
RiskDescription: Unauthorized external connections and data breaches resulting from split tunneling ca
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and monitoring for remote devices", "2": "Regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1725:
RiskId: 1057
ComplianceId: 1080
RiskTitle: Unauthorized Access to Internal Communications Traffic
Criticality: High
PossibleDamage: Unauthorized access to sensitive internal communications, potential data breaches,
Category: Operational
RiskType: Current
BusinessImpact: All business units within the organization
RiskDescription: Unauthorized access to internal communications traffic can lead to data breaches, co
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strong authentication mechanisms for proxy servers", "2": "Regularly m

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 1726:

RiskId: 1058

ComplianceId: 1081

RiskTitle: Access to Unauthorized Websites

Criticality: Medium

PossibleDamage: Access to unauthorized websites, exposure to malicious content, increased risk of m

Category: Operational

RiskType: Current

BusinessImpact: All business units within the organization

RiskDescription: Access to unauthorized websites can lead to exposure to malicious content, increase

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly update and maintain the list of authorized and unauthorized websites",

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1727:

RiskId: 1059

ComplianceId: 1082

RiskTitle: Failure to Implement Host-based Boundary Protection Mechanisms

Criticality: High

PossibleDamage: Unauthorized access, data breaches, malware infections

Category: IT
RiskType: Residual
BusinessImpact: Potential breaches and data loss affecting all business units
RiskDescription: Failure to implement host-based boundary protection mechanisms may lead to unautl
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and patch host-based protection mechanisms", "2": "Monitor an
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1728:
RiskId: 1060
ComplianceId: 1083
RiskTitle: Data Breach Due to Boundary Protection Failure
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal consequences, damage to reputation
RiskDescription: Failure to implement fail-secure mechanisms may lead to unauthorized access to sen
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and maintenance of boundary protection devices", "2": "Implemen
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1729:
RiskId: 1061
ComplianceId: 1084
RiskTitle: Risk of Unencrypted Transmission
Criticality: High
PossibleDamage: Unauthorized access or modification of sensitive information
Category: IT
RiskType: Current
BusinessImpact: Loss of confidentiality and integrity of transmitted information
RiskDescription: Failure to encrypt transmitted information may result in unauthorized access or modifi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption algorithms", "2": "Regularly update encryption keys",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1730:
RiskId: 1062
ComplianceId: 1085
RiskTitle: Risk of Unprotected Transmission of Classified Information
Criticality: Critical
PossibleDamage: Unauthorized access to classified information, compromise of national security
Category: Operational
RiskType: Current
BusinessImpact: Compromise of national security, loss of classified information
RiskDescription: Failure to utilize protected distribution systems for classified information transmission

RiskLikelihood: 7
RiskImpact: 10
RiskExposureRating: 70
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement physical controls for protected distribution systems", "2": "Regularly au
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1731:
RiskId: 1063
ComplianceId: 1086
RiskTitle: Data Interception Risk
Criticality: High
PossibleDamage: Unauthorized access or modification of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of data confidentiality and integrity, potential legal implications
RiskDescription: The risk of data interception during transmission leading to unauthorized access or m
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption algorithms", "2": "Regularly update cryptographic ke
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1732:
RiskId: 1064

ComplianceId: 1087
RiskTitle: Data Integrity Compromise Risk
Criticality: Medium
PossibleDamage: Incorrect data processing or decision-making
Category: Operational
RiskType: Residual
BusinessImpact: Loss of data integrity, potential operational disruptions
RiskDescription: The risk of data integrity compromise during transmission leading to incorrect data pro
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement data validation checks", "2": "Establish data integrity monitoring proces
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1733:
RiskId: 1065
ComplianceId: 1088
RiskTitle: Unauthorized Network Access
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties, legal repercussions
RiskDescription: Unauthorized access to network resources due to failure to disconnect sessions in a t
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement automated network disconnect mechanisms", "2": "Regularly monitor r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1734:
RiskId: 1066
ComplianceId: 1089
RiskTitle: Resource Contention
Criticality: Medium
PossibleDamage: Degraded application performance, potential downtime
Category: IT
RiskType: Current
BusinessImpact: Loss of productivity, increased support costs
RiskDescription: Resource conflicts due to multiple application sessions using a single network connec
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement application-level network management tools", "2": "Regularly review ar
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1735:
RiskId: 1067
ComplianceId: 1090
RiskTitle: Weak Encryption Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data

Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, reputational damage, regulatory fines
RiskDescription: Failure to comply with key generation requirements may result in weak encryption, ma
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong cryptographic algorithms for key generation", "2": "Regularly rev
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1736:
RiskId: 1068
ComplianceId: 1091
RiskTitle: Key Distribution and Storage Risk
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive data
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches, loss of sensitive data, reputational damage
RiskDescription: Failure to comply with key distribution and storage requirements may result in unauth
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement secure protocols for key distribution", "2": "Encrypt keys at rest to prote
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1737:
RiskId: 1069
ComplianceId: 1092
RiskTitle: Unauthorized Access to Classified Information
Criticality: High
PossibleDamage: Compromise of sensitive data, legal implications, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of trust, financial penalties, legal consequences
RiskDescription: Unauthorized individuals gaining access to classified information due to improper cryp
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls", "2": "Regularly review and update cryptograph
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 1738:
RiskId: 1070
ComplianceId: 1093
RiskTitle: Data Leakage due to Incorrect Cryptographic Implementation
Criticality: Medium
PossibleDamage: Loss of sensitive data, legal implications, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal consequences, reputational damage
RiskDescription: Improper implementation of cryptography leading to data leakage and unauthorized a

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update cryptographic implementations", "2": "Conduct regular security a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1739:
RiskId: 1071
ComplianceId: 1094
RiskTitle: Unauthorized Remote Activation
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, invasion of privacy
Category: Operational
RiskType: Current
BusinessImpact: Data breaches, loss of trust
RiskDescription: Unauthorized remote activation could lead to unauthorized access to confidential mee
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication controls for remote activation", "2": "Regularly re
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1740:
RiskId: 1072

ComplianceId: 1095
RiskTitle: Lack of Explicit Indication of Use
Criticality: Medium
PossibleDamage: Unintended recording or monitoring of individuals
Category: Legal
RiskType: Current
BusinessImpact: Legal consequences and reputational damage
RiskDescription: Failure to provide explicit indication of use could lead to unintended recording or moni
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement visual indicators (LED lights) when devices are active", "2": "Train user
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1741:
RiskId: 1073
ComplianceId: 1096
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, loss of confidential information
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Unauthorized access to sensitive information due to compromised public key certificat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement access controls based on certificate policies", "2": "Regularly monitor a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1742:
RiskId: 1074
ComplianceId: 1097
RiskTitle: Compromised System Integrity
Criticality: Medium
PossibleDamage: Data integrity violations, system malfunctions
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, reputational damage
RiskDescription: Inclusion of unauthorized trust anchors leading to compromised system integrity and t
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement strict access controls for trust store management", "2": "Regularly revie
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1743:
RiskId: 1075
ComplianceId: 1098
RiskTitle: Unauthorized Execution of Malicious Mobile Code
Criticality: High
PossibleDamage: System compromise, data loss, unauthorized access

Category: IT
RiskType: Current
BusinessImpact: Potential disruption of operations, loss of sensitive data, reputational damage
RiskDescription: Unauthorized execution of malicious mobile code could lead to system compromise, d
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and enforce the list of acceptable mobile code and technologies
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1744:
RiskId: 1076
ComplianceId: 1099
RiskTitle: Unauthorized or Malicious Use of Mobile Code
Criticality: High
PossibleDamage: System compromise, data loss, unauthorized access
Category: IT
RiskType: Current
BusinessImpact: Potential disruption of operations, loss of sensitive data, reputational damage
RiskDescription: Unauthorized or malicious use of mobile code could lead to system compromise, data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls to restrict who can execute mobile code", "2": "Monito
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1745:
RiskId: 1077
ComplianceId: 1100
RiskTitle: Unauthorized Access to Network Resources
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, potential data breaches
Category: IT
RiskType: Current
BusinessImpact: Loss of data confidentiality, potential financial losses
RiskDescription: Unauthorized users gaining access to sensitive network resources and data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls", "2": "Regularly audit access logs", "3": "Imple
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1746:
RiskId: 1078
ComplianceId: 1101
RiskTitle: Trust Relationship Compromises
Criticality: High
PossibleDamage: Unauthorized zone modifications, potential DNS hijacking
Category: IT
RiskType: Current
BusinessImpact: Loss of trust in domain resolution, potential service disruptions
RiskDescription: Compromised trust relationships leading to unauthorized modifications in child zones

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement DNSSEC for child zones", "2": "Regularly audit zone configurations", "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1747:
RiskId: 1079
ComplianceId: 1102
RiskTitle: Unauthorized Data Access and Manipulation
Criticality: High
PossibleDamage: Potential unauthorized access or data manipulation due to unauthenticated or comp
Category: IT
RiskType: Current
BusinessImpact: Disruption of services, data breaches, loss of trust
RiskDescription: Failure to authenticate and verify resolution responses can lead to unauthorized acce
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement DNSSEC for DNS resolution", "2": "Use trusted validation providers fo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1748:
RiskId: 1080

ComplianceId: 1103
RiskTitle: Service Disruption Due to DNS Server Failure
Criticality: High
PossibleDamage: Service downtime, data loss, reputation damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of revenue, customer dissatisfaction
RiskDescription: Failure of primary DNS server leading to service disruption and potential data loss
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated failover mechanisms", "2": "Regularly test failover procedur
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1749:
RiskId: 1081
ComplianceId: 1104
RiskTitle: Unauthorized Access to Internal DNS Information
Criticality: Medium
PossibleDamage: Data breach, exposure of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Loss of confidential data, regulatory fines
RiskDescription: Unauthorized external access to internal DNS server containing sensitive information
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement strict access controls based on roles", "2": "Regularly audit DNS serve
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1750:
RiskId: 1082
ComplianceId: 1105
RiskTitle: Session Authenticity Breach
Criticality: High
PossibleDamage: Loss of sensitive information, compromised communication integrity, reputational da
Category: Operational
RiskType: Current
BusinessImpact: Loss of trust, financial losses, legal implications
RiskDescription: Unauthorized access to communication sessions can lead to leakage of confidential i
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement end-to-end encryption for all communication sessions", "2": "Use multi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1751:
RiskId: 1083
ComplianceId: 1106
RiskTitle: Unauthorized Access to User Information at Rest
Criticality: High
PossibleDamage: Data breaches, financial losses, and reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: All business units handling user information would be impacted by potential data brea
RiskDescription: Unauthorized access to sensitive user information stored at rest could lead to data br
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption mechanisms for user information at rest", "2": "Enfor
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1752:
RiskId: 1084
ComplianceId: 1107
RiskTitle: Unauthorized Alterations to System Information at Rest
Criticality: Medium
PossibleDamage: System vulnerabilities, security breaches, and potential data loss
Category: IT
RiskType: Residual
BusinessImpact: IT and security departments responsible for system configurations and rule sets woul
RiskDescription: Unauthorized alterations to system-related information stored at rest could lead to sys
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement write-once-read-many (WORM) technologies for system-related inform
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1753:
RiskId: 1085
ComplianceId: 1108
RiskTitle: Data Breach Due to Inadequate Cryptographic Protection
Criticality: High
PossibleDamage: Financial loss, reputational damage, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust, regulatory fines
RiskDescription: Failure to implement strong cryptographic mechanisms may lead to unauthorized acc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular encryption key rotation", "2": "Implementation of strong encryption algorit
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1754:
RiskId: 1086
ComplianceId: 1109
RiskTitle: Security Vulnerabilities due to Process Isolation Failure
Criticality: High
PossibleDamage: Unauthorized access, data leakage, system compromise
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, system downtime, reputational damage
RiskDescription: Failure to maintain process isolation could lead to unauthorized access to critical syst

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls", "2": "Regularly monitor system activity", "3": "Im
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1755:
RiskId: 1087
ComplianceId: 1110
RiskTitle: Unsynchronized System Clocks
Criticality: High
PossibleDamage: Denial of service, unauthorized access, security breaches
Category: Operational
RiskType: Current
BusinessImpact: Loss of data, system downtime, reputational damage
RiskDescription: Failure to synchronize system clocks may lead to security vulnerabilities and unautho
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated time synchronization tools", "2": "Regularly monitor and au
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1756:
RiskId: 1088

ComplianceId: 1111
RiskTitle: Inconsistent Time Stamps
Criticality: High
PossibleDamage: Data discrepancies and operational inefficiencies
Category: Operational
RiskType: Current
BusinessImpact: Data discrepancies could lead to financial losses and regulatory non-compliance
RiskDescription: Failure to compare internal system clocks with the authoritative time source can resul
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated clock comparison tools", "2": "Regularly monitor clock comp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1757:
RiskId: 1089
ComplianceId: 1112
RiskTitle: Inaccurate Time Synchronization
Criticality: Medium
PossibleDamage: Transaction failures and audit issues
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate time synchronization could lead to transaction failures, audit issues, and c
RiskDescription: Failure to synchronize internal system clocks with the authoritative time source can re
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Automate clock synchronization process", "2": "Implement real-time monitoring fo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1758:
RiskId: 1090
ComplianceId: 1113
RiskTitle: Inadequate System and Information Integrity Policy
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats and potential data breaches
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive data, reputational damage, financial losses
RiskDescription: Failure to have a robust system and information integrity policy may expose the orgar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly update security patches an
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1759:
RiskId: 1091
ComplianceId: 1114
RiskTitle: Lack of Designated System and Information Integrity Policy Manager
Criticality: Medium
PossibleDamage: Inconsistent policy management and oversight

Category: Operational
RiskType: Current
BusinessImpact: Policy inconsistencies, lack of accountability
RiskDescription: Failure to designate an official to manage the system and information integrity policy r
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting lines and escalation procedures", "2": "Provide regular p
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1760:
RiskId: 1092
ComplianceId: 1115
RiskTitle: Outdated System and Information Integrity Policy and Procedures
Criticality: Low
PossibleDamage: Non-alignment with current security threats and regulatory requirements
Category: Compliance
RiskType: Current
BusinessImpact: Non-compliance with regulations, increased security risks
RiskDescription: Failure to review and update system and information integrity policy and procedures r
RiskLikelihood: 5
RiskImpact: 4
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Establish regular policy review schedules", "2": "Conduct periodic policy gap analy
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1761:
RiskId: 1093
ComplianceId: 1116
RiskTitle: Failure to Identify and Remediate System Flaws
Criticality: High
PossibleDamage: Unauthorized access, data breaches, system compromise
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to identify and remediate system flaws may result in unauthorized access to s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular vulnerability scanning and assessment tools", "2": "Establish cl
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1762:
RiskId: 1094
ComplianceId: 1117
RiskTitle: Failure to Test Software and Firmware Updates
Criticality: Medium
PossibleDamage: System instability, compatibility issues, security vulnerabilities
Category: Operational
RiskType: Inherent
BusinessImpact: IT and security teams
RiskDescription: Failure to test software and firmware updates may lead to system instability, compatib

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a comprehensive testing environment for updates", "2": "Implement auto
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1763:
RiskId: 1095
ComplianceId: 1118
RiskTitle: Delay in Installing Security Updates
Criticality: High
PossibleDamage: System compromise, data breaches, unauthorized access
Category: Operational
RiskType: Inherent
BusinessImpact: IT operations and system administrators
RiskDescription: Delay in installing security updates may expose systems to known vulnerabilities, lead
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish automated update deployment processes", "2": "Implement patch mana
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1764:
RiskId: 1096

ComplianceId: 1119
RiskTitle: Exploitation of Unpatched Vulnerabilities
Criticality: High
PossibleDamage: Data breaches, system compromise, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, disruption of operations, reputational damage
RiskDescription: Failure to detect and remediate known flaws in system components may allow attacke
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated patch management systems", "2": "Regularly update autom
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1765:
RiskId: 1097
ComplianceId: 1120
RiskTitle: Delayed Flaw Remediation
Criticality: High
PossibleDamage: Increased vulnerability and potential exploitation
Category: IT
RiskType: Current
BusinessImpact: Potential system breaches, data loss, and reputational damage
RiskDescription: Failure to remediate system flaws in a timely manner can expose the organization to s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement automated flaw remediation processes", "2": "Regularly review and up
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1766:
RiskId: 1098
ComplianceId: 1121
RiskTitle: Inadequate Corrective Action Benchmarks
Criticality: Medium
PossibleDamage: Delays in flaw remediation and increased vulnerability
Category: Operational
RiskType: Current
BusinessImpact: Operational inefficiencies, security risks, and compliance violations
RiskDescription: Lack of clear benchmarks for corrective actions can lead to inconsistent practices and
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update benchmarks based on evolving threat landscape", "2
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1767:
RiskId: 1099
ComplianceId: 1122
RiskTitle: Data Breach and System Compromise
Criticality: High
PossibleDamage: Data breaches, compromised sensitive information, system downtime

Category: IT
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial losses, damage to reputation
RiskDescription: Malicious code entering the system undetected could lead to data breaches, compron
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update malicious code protection mechanisms", "2": "Conduct periodic
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1768:
RiskId: 1100
ComplianceId: 1123
RiskTitle: Outdated Protection Mechanisms
Criticality: Medium
PossibleDamage: System compromise, data breaches, compromised sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Potential system downtime, financial losses, damage to reputation
RiskDescription: Failure to update protection mechanisms may result in the inability to detect and erad
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly check for updates to malicious code protection mechanisms", "2": "Auto
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1769:
RiskId: 1101
ComplianceId: 1124
RiskTitle: Undetected Malicious Code
Criticality: High
PossibleDamage: Data breaches, compromised sensitive information, system compromise
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial losses, damage to reputation
RiskDescription: Failure to configure protection mechanisms may result in undetected malicious code e
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Define organization-specific scan frequencies", "2": "Implement real-time scanning
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1770:
RiskId: 1102
ComplianceId: 1125
RiskTitle: Potential Data Breach
Criticality: High
PossibleDamage: Loss of sensitive information, reputational damage, legal consequences
Category: IT
RiskType: Current
BusinessImpact: Disruption of business operations, financial losses, regulatory fines
RiskDescription: Unauthorized access to sensitive data due to ineffective monitoring

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for sensitive data", "2": "Implement multi-factor authenticati
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1771:
RiskId: 1103
ComplianceId: 1126
RiskTitle: Unauthorized System Access
Criticality: Medium
PossibleDamage: Compromised system integrity, data leaks, legal consequences
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive data, disruption of business operations, reputational damage
RiskDescription: Unauthorized users gaining access to critical system resources
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement strong authentication mechanisms", "2": "Regularly review user access
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1772:
RiskId: 1104

ComplianceId: 1127
RiskTitle: Legal Non-Compliance
Criticality: High
PossibleDamage: Regulatory fines, lawsuits, reputational damage
Category: Legal
RiskType: Current
BusinessImpact: Legal consequences, financial losses, reputational damage
RiskDescription: Failure to obtain legal opinion on system monitoring activities leading to legal non-com
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Engage legal counsel for compliance reviews", "2": "Implement legal compliance t
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1773:
RiskId: 1105
ComplianceId: 1128
RiskTitle: Increased Vulnerability to Cyber Attacks
Criticality: High
PossibleDamage: Potential data breaches and financial losses
Category: IT
RiskType: Residual
BusinessImpact: Disruption of critical systems and loss of sensitive data
RiskDescription: Failure to integrate individual intrusion detection tools into a system-wide IDS may lea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and updating of intrusion detection tools", "2": "Implementing
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1774:
RiskId: 1106
ComplianceId: 1129
RiskTitle: Failure to Implement Automated Monitoring Tools
Criticality: High
PossibleDamage: Delayed incident response, potential data breaches, unauthorized access
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to implement automated monitoring tools may result in delayed detection of se
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and maintain automated monitoring tools", "2": "Conduct regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1775:
RiskId: 1107
ComplianceId: 1130
RiskTitle: Failure to Detect Malicious Activities in Communications Traffic
Criticality: High
PossibleDamage: Data breaches, system compromise, unauthorized access to sensitive information

Category: Operational
RiskType: Inherent
BusinessImpact: Potential loss of sensitive data, damage to reputation, financial losses
RiskDescription: The risk of failing to detect malicious activities in inbound and outbound communicatio
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust monitoring tools and technologies", "2": "Regularly review and u
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1776:
RiskId: 1108
ComplianceId: 1131
RiskTitle: Failure to Monitor Communications Traffic
Criticality: Medium
PossibleDamage: Undetected security incidents, data breaches, unauthorized access
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of services, loss of sensitive data, reputational damage
RiskDescription: The risk of not monitoring inbound and outbound communications traffic could lead to
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated monitoring tools with real-time alerts", "2": "Establish incide
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1777:
RiskId: 1109
ComplianceId: 1132
RiskTitle: Failure to Detect Compromises
Criticality: High
PossibleDamage: Data breaches, system downtime, unauthorized access
Category: Operational
RiskType: Residual
BusinessImpact: Significant financial and reputational damage
RiskDescription: If compromises go undetected, sensitive data could be exposed, systems could be dis
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated alerting systems", "2": "Regularly update compromise indic
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1778:
RiskId: 1110
ComplianceId: 1133
RiskTitle: Delayed Incident Response
Criticality: Medium
PossibleDamage: Increased impact of security incidents
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions and potential data loss
RiskDescription: If key personnel are not promptly notified of security alerts, incidents may escalate, le

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update alert notification list", "2": "Ensure clear roles and res
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1779:
RiskId: 1111
ComplianceId: 1134
RiskTitle: Undetected Attack Patterns
Criticality: High
PossibleDamage: Undetected attack patterns may lead to security breaches and data compromise.
Category: Operational
RiskType: Residual
BusinessImpact: IT, Security, Operations
RiskDescription: Failure to correlate monitoring information may result in undetected attack patterns, le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated correlation tools", "2": "Regularly review and analyze correl
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1780:
RiskId: 1112

ComplianceId: 1135
RiskTitle: Covert Exfiltration of Information
Criticality: High
PossibleDamage: Loss of sensitive information and data breach
Category: Operational
RiskType: Current
BusinessImpact: Loss of reputation, legal consequences
RiskDescription: Unauthorized transfer of sensitive information through outbound communications traff
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement data loss prevention tools", "2": "Regularly monitor outbound traffic", "3
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1781:
RiskId: 1113
ComplianceId: 1136
RiskTitle: Covert Exfiltration through Interior Points
Criticality: Medium
PossibleDamage: Unauthorized data exfiltration and compromise of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, regulatory fines
RiskDescription: Unauthorized transfer of sensitive information through internal system points
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement intrusion detection systems", "2": "Regularly audit internal network traf
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1782:
RiskId: 1114
ComplianceId: 1137
RiskTitle: Security Breach Due to Lack of Host-based Monitoring
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, financial loss, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Financial loss, reputational damage, legal consequences
RiskDescription: Failure to implement host-based monitoring mechanisms may lead to undetected sec
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and patch host-based monitoring tools", "2": "Conduct regular a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1783:
RiskId: 1115
ComplianceId: 1138
RiskTitle: Monitoring Gaps Due to Single Vendor Dependency
Criticality: Medium
PossibleDamage: Blind spots in monitoring, delayed threat detection, increased vulnerability to attacks

Category: IT
RiskType: Residual
BusinessImpact: Increased risk of security incidents, potential data breaches
RiskDescription: Relying solely on one vendor's monitoring tools may result in blind spots in monitoring
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly assess and compare the effectiveness of different monitoring tools", "2"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1784:
RiskId: 1116
ComplianceId: 1139
RiskTitle: Failure to Receive Security Alerts and Directives
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats, potential breaches, and operational disruptio
Category: Operational
RiskType: Inherent
BusinessImpact: Potential breaches could lead to financial losses, reputational damage, and legal impl
RiskDescription: Failure to receive timely security alerts and directives may result in delayed response
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish automated alert systems for timely notification", "2": "Regularly monitor
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 1785:
RiskId: 1117
ComplianceId: 1140
RiskTitle: Failure to Disseminate Security Alerts and Directives
Criticality: Medium
PossibleDamage: Stakeholders being unaware of critical information, increased vulnerability to cyber t
Category: Operational
RiskType: Inherent
BusinessImpact: Miscommunication could lead to ineffective response to threats and potential breache
RiskDescription: Failure to disseminate security alerts and directives may result in stakeholders being
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels for dissemination", "2": "Provide training
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1786:
RiskId: 1118
ComplianceId: 1141
RiskTitle: Unauthorized Access and Privacy Breach Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, privacy breaches
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, damage to reputation
RiskDescription: Failure to verify security and privacy functions may lead to unauthorized access to se

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and verification of security and privacy functions", "2": "Implement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1787:
RiskId: 1119
ComplianceId: 1142
RiskTitle: System Instability Risk
Criticality: Medium
PossibleDamage: System instability, unexpected system shutdowns
Category: Operational
RiskType: Residual
BusinessImpact: Potential system downtime and disruption to operations
RiskDescription: Failure to verify system transitional states may lead to system instability or unexpecte
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular testing of system transitional states", "2": "Implementing automated moni
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1788:
RiskId: 1120

ComplianceId: 1143
RiskTitle: Unauthorized Changes Detection Failure
Criticality: High
PossibleDamage: System compromise, data breaches, loss of sensitive information.
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, reputational damage.
RiskDescription: Failure to detect unauthorized changes could result in severe consequences for the o
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement continuous monitoring tools", "2": "Establish incident response procedu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1789:
RiskId: 1121
ComplianceId: 1144
RiskTitle: Delayed Response to Unauthorized Changes
Criticality: Medium
PossibleDamage: Extended system vulnerabilities, data exposure, regulatory fines.
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties, operational disruptions.
RiskDescription: Delayed response to unauthorized changes can exacerbate security risks and lead to
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Automate incident response processes", "2": "Establish clear escalation paths", "3

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1790:

RiskId: 1122

ComplianceId: 1145

RiskTitle: Unauthorized System Access

Criticality: High

PossibleDamage: Potential unauthorized access or compromise of system integrity

Category: IT

RiskType: Residual

BusinessImpact: All business units would be impacted by unauthorized access

RiskDescription: Unauthorized access to sensitive information, malware installation, system compromis

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement secure boot mechanisms", "2": "Regularly update integrity check softw

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 1791:

RiskId: 1123

ComplianceId: 1146

RiskTitle: System Compromise during Critical Events

Criticality: Critical

PossibleDamage: Potential system instability or compromise during critical events

Category: IT
RiskType: Residual
BusinessImpact: Critical business units would be impacted by system compromise
RiskDescription: System compromise during critical events, data loss, service disruption
RiskLikelihood: 9
RiskImpact: 10
RiskExposureRating: 90
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement real-time monitoring tools", "2": "Establish incident response procedure
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1792:
RiskId: 1124
ComplianceId: 1147
RiskTitle: Compromised System Integrity
Criticality: High
PossibleDamage: Data breaches, legal actions
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of sensitive data
RiskDescription: Unauthorized changes to system settings or privileges could lead to system vulnerabi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls", "2": "Regularly update security patches", "3": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1793:
RiskId: 1125
ComplianceId: 1148
RiskTitle: Increased Risk of Malware Infections and Data Breaches
Criticality: High
PossibleDamage: Data loss, financial losses, reputational damage.
Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, loss of sensitive data, financial repercussions.
RiskDescription: Failure to implement spam protection mechanisms may lead to an increased risk of m
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update spam protection mechanisms", "2": "Implement email filtering ru
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 1794:
RiskId: 1126
ComplianceId: 1149
RiskTitle: Increased Spam Exposure
Criticality: High
PossibleDamage: Potential phishing attacks, malware infections, and data breaches
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of sensitive data, financial losses, damage to reputation
RiskDescription: Failure to update spam protection mechanisms regularly may lead to an increased ex

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated update schedules with notifications to IT administrators", "2
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1795:
RiskId: 1127
ComplianceId: 1150
RiskTitle: Data Corruption and Unauthorized Access Risk
Criticality: High
PossibleDamage: Data loss, system downtime, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Invalid inputs can lead to data corruption or unauthorized access, compromising syste
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict input validation rules", "2": "Regularly monitor and audit system i
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1796:
RiskId: 1128

ComplianceId: 1151
RiskTitle: Disclosure of Sensitive Information
Criticality: High
PossibleDamage: Data breaches, unauthorized access, identity theft
Category: Compliance
RiskType: Residual
BusinessImpact: Potential loss of customer trust, legal implications
RiskDescription: Unauthorized access to sensitive information through error messages could lead to da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement generic error messages without specific details", "2": "Encrypt sensitive
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1797:
RiskId: 1129
ComplianceId: 1152
RiskTitle: Unauthorized Access to Error Messages
Criticality: Medium
PossibleDamage: Data leaks, insider threats
Category: Operational
RiskType: Residual
BusinessImpact: Potential compromise of sensitive information, operational disruptions
RiskDescription: Unauthorized personnel accessing error messages could lead to data leaks and insid
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement role-based access control for error messages", "2": "Regularly review a

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1798:

RiskId: 1130

ComplianceId: 1153

RiskTitle: Non-Compliance with Information Retention

Criticality: High

PossibleDamage: Legal penalties, loss of critical information, reputational damage.

Category: Compliance

RiskType: Current

BusinessImpact: Loss of critical information, regulatory fines, reputational damage.

RiskDescription: Failure to retain information output from controls can lead to legal and regulatory non-

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular audits to ensure compliance", "2": "Training sessions for employees on re

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 1799:

RiskId: 1131

ComplianceId: 1154

RiskTitle: Unauthorized Code Execution Risk

Criticality: High

PossibleDamage: Unauthorized code execution leading to system compromise or data breach

Category: IT
RiskType: Current
BusinessImpact: All business units would be impacted by a potential breach
RiskDescription: The risk of unauthorized code execution poses a significant threat to the confidentialit
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and patch systems to address vulnerabilities", "2": "Implement n
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1800:
RiskId: 1132
ComplianceId: 1155
RiskTitle: Code Execution Attack Risk
Criticality: High
PossibleDamage: Successful code execution attacks leading to system compromise
Category: IT
RiskType: Current
BusinessImpact: All business units would be impacted by a potential breach
RiskDescription: The risk of successful code execution attacks can result in unauthorized access, data
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and patch systems to address vulnerabilities", "2": "Implement n
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1801:
RiskId: 1133
ComplianceId: 1156
RiskTitle: Non-compliance with Supply Chain Risk Management Policy
Criticality: High
PossibleDamage: Increased vulnerability to supply chain risks, potential breaches, and non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face disruptions, financial losses, and reputational damage
RiskDescription: Failure to comply with the supply chain risk management policy may expose the orga
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on supply chain risk management", "2"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1802:
RiskId: 1134
ComplianceId: 1157
RiskTitle: Lack of Designated Official for Supply Chain Risk Management Policy
Criticality: Medium
PossibleDamage: Confusion, delays, and inconsistencies in policy management
Category: Operational
RiskType: Inherent
BusinessImpact: Policy management may lack oversight and accountability, leading to inefficiencies ar
RiskDescription: Without a designated official, there may be confusion in policy management, delays in

RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clearly define roles and responsibilities of the designated official", "2": "Provide ad
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1803:
RiskId: 1135
ComplianceId: 1158
RiskTitle: Non-compliance with Updated Supply Chain Risk Management Policy and Procedures
Criticality: High
PossibleDamage: Vulnerabilities, non-compliance, and increased risks
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may face increased risks and non-compliance issues
RiskDescription: Failure to review and update supply chain risk management policy and procedures ma
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a regular review schedule for policy and procedure updates", "2": "Enga
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1804:
RiskId: 1136

ComplianceId: 1159
RiskTitle: Failure to develop a supply chain risk management plan
Criticality: High
PossibleDamage: Increased security and privacy risks in the supply chain
Category: Operational
RiskType: Current
BusinessImpact: Disruption of supply chain operations, potential loss of sensitive information
RiskDescription: Failure to develop a comprehensive plan for managing supply chain risks may lead to
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of the plan", "2": "Incorporating feedback from stakeho
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1805:
RiskId: 1137
ComplianceId: 1160
RiskTitle: Outdated supply chain risk management plan
Criticality: Medium
PossibleDamage: Plan may not address current threats and risks in the supply chain
Category: Operational
RiskType: Current
BusinessImpact: Ineffective risk mitigation strategies, increased vulnerability to supply chain risks
RiskDescription: An outdated supply chain risk management plan may not address new threats and ris
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regular review schedule", "2": "Incorporating feedback from stakeholders", "3": "T

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1806:

RiskId: 1138

ComplianceId: 1161

RiskTitle: Ineffective SCRM Team Establishment

Criticality: High

PossibleDamage: Supply chain disruptions, security breaches, legal liabilities

Category: Operational

RiskType: Residual

BusinessImpact: Disruption of supply chain operations, compromised data security, legal consequence

RiskDescription: Failure to establish a SCRM team with defined roles and responsibilities may lead to i

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Define clear roles and responsibilities for each SCRM team member", "2": "Provid

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: IT Operations Unit

Item 1807:

RiskId: 1139

ComplianceId: 1162

RiskTitle: Supply Chain Weakness Exploitation

Criticality: High

PossibleDamage: Adversaries exploiting weaknesses in the supply chain could lead to significant harm

Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, compromised system integrity, reputational damage
RiskDescription: Adversaries exploiting weaknesses in the supply chain could introduce malicious com
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular vulnerability assessments", "2": "Continuous monitoring of supply chain p
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1808:
RiskId: 1140
ComplianceId: 1163
RiskTitle: Supply Chain Risk Impact
Criticality: Medium
PossibleDamage: Supply chain risks could lead to system compromise, data breaches, or service disru
Category: Operational
RiskType: Current
BusinessImpact: System compromise, data breaches, service disruptions
RiskDescription: Failure to implement supply chain controls could result in supply chain risks causing h
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update of supply chain controls", "2": "Integration of supply ch
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1809:
RiskId: 1141
ComplianceId: 1164
RiskTitle: Supply Chain Risks Due to Lack of Acquisition Strategy Implementation
Criticality: High
PossibleDamage: Unauthorized production, theft, tampering, insertion of counterfeits, insertion of malic
Category: Operational
RiskType: Inherent
BusinessImpact: All business units would be impacted by supply chain risks
RiskDescription: Failure to implement acquisition strategies, tools, and methods may lead to significant
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for personnel on supply chain risk mitig
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1810:
RiskId: 1142
ComplianceId: 1165
RiskTitle: Supplier Risk Assessment Frequency
Criticality: High
PossibleDamage: Failure to conduct regular assessments may result in increased exposure to security
Category: Operational
RiskType: Residual
BusinessImpact: All business units may face operational disruptions and financial losses.
RiskDescription: Inadequate supplier risk assessments can lead to vulnerabilities in the supply chain, p

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated risk assessment tools", "2": "Enhance supplier monitoring p
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1811:
RiskId: 1143
ComplianceId: 1166
RiskTitle: Delayed Response to Supply Chain Compromises
Criticality: High
PossibleDamage: Data breaches, system failures
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, disruption of operations
RiskDescription: Failure to establish notification agreements may result in delayed response to supply
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update notification agreements", "2": "Conduct regular traini
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1812:
RiskId: 1144

ComplianceId: 1167
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information
Category: IT
RiskType: Inherent
BusinessImpact: Potential data breach, loss of confidential information
RiskDescription: Unauthorized individuals gaining access to sensitive data due to tampering with syste
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Encrypt sensitive data", "3": "Regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1813:
RiskId: 1145
ComplianceId: 1168
RiskTitle: Delayed Response Risk
Criticality: Medium
PossibleDamage: Delayed response to tampering incidents
Category: IT
RiskType: Inherent
BusinessImpact: Potential security breaches, compromised system integrity
RiskDescription: Failure to promptly respond to tampering indications leading to unauthorized access c
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish automated tamper detection alerts", "2": "Regularly update tamper dete

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 1814:

RiskId: 1146

ComplianceId: 1169

RiskTitle: Introduction of Counterfeit Components

Criticality: High

PossibleDamage: System vulnerabilities, data breaches, compromised system integrity.

Category: Operational

RiskType: Current

BusinessImpact: Potential data loss, system downtime, financial losses.

RiskDescription: The risk of counterfeit components entering the system poses a significant threat to s

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular supplier audits to verify component authenticity", "2": "Implementation of

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 1815:

RiskId: 1147

ComplianceId: 1170

RiskTitle: Failure to Report Counterfeit Components

Criticality: Medium

PossibleDamage: Further distribution of counterfeit components, compromised system integrity.

Category: Compliance
RiskType: Current
BusinessImpact: Legal implications, reputational damage, loss of customer trust.
RiskDescription: Failure to report counterfeit components could result in legal consequences and comp
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting procedures for counterfeit components", "2": "Regular tra
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1816:
RiskId: 1148
ComplianceId: 1171
RiskTitle: Risk of Deploying Counterfeit System Components
Criticality: High
PossibleDamage: Deployment of counterfeit components leading to system failure, security breaches,
Category: Operational
RiskType: Inherent
BusinessImpact: Procurement delays, financial losses, reputational damage.
RiskDescription: The risk of unknowingly deploying counterfeit system components can have severe co
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on counterfeit detection techniques", "2": "Implementing
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1817:
RiskId: 1149
ComplianceId: 1172
RiskTitle: Unauthorized Access to System Components
Criticality: High
PossibleDamage: Data breaches, system downtime, operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, financial losses, reputational damage
RiskDescription: Unauthorized access to system components can lead to unauthorized modifications, d
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls and monitoring for components in service or repair", "2
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1818:
RiskId: 1150
ComplianceId: 1173
RiskTitle: Unauthorized Access to Disposed Components
Criticality: High
PossibleDamage: Data breaches, intellectual property theft
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, legal consequences
RiskDescription: Unauthorized individuals gaining access to disposed components containing sensitive

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement secure disposal procedures", "2": "Regularly train employees on prope
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1819:
RiskId: 1151
ComplianceId: 1174
RiskTitle: Confidential Information Disclosure
Criticality: Medium
PossibleDamage: Regulatory non-compliance, data leaks
Category: Operational
RiskType: Current
BusinessImpact: Legal consequences, loss of reputation
RiskDescription: Unauthorized individuals gaining access to disposed documentation containing confid
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement document shredding policies", "2": "Encrypt sensitive documents befor
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1820:
RiskId: 427

ComplianceId: 439
RiskTitle: Lack of Climate-related Risk Assessment
Criticality: High
PossibleDamage: Financial losses, missed strategic opportunities, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, reputational damage, regulatory non-compliance
RiskDescription: Failure to conduct annual assessment of climate-related risks may leave the organiza
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for Risk Management Department on climate-related risk assess
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1821:
RiskId: 428
ComplianceId: 440
RiskTitle: Financial Losses from Unanticipated Climate Impacts
Criticality: High
PossibleDamage: Financial losses due to unanticipated climate-related impacts on budgeting
Category: Financial
RiskType: Inherent
BusinessImpact: Potential negative impact on financial performance and sustainability
RiskDescription: Failure to incorporate climate risks in budgeting may lead to inaccurate financial forec
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular climate risk assessments during budgeting process", "2": "Scenario plann
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1822:
RiskId: 429
ComplianceId: 441
RiskTitle: Reputational Damage from Lack of Climate Reporting
Criticality: Medium
PossibleDamage: Reputational damage due to lack of transparency and accountability in addressing c
Category: Reputational
RiskType: Inherent
BusinessImpact: Potential negative impact on stakeholder trust, regulatory compliance, and brand repu
RiskDescription: Failure to report on climate considerations in financial planning may lead to stakehold
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting mechanisms and templates for climate considerations", "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1823:
RiskId: 430
ComplianceId: 442
RiskTitle: Failure to Conduct Annual Climate Risk Assessment
Criticality: High
PossibleDamage: Inadequate identification and mitigation of climate-related risks, leading to financial l

Category: Environmental
RiskType: Inherent
BusinessImpact: All business units may be impacted by climate-related risks
RiskDescription: Failure to conduct annual climate risk assessments may result in inadequate identifica
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training programs for risk management team on climate risk as
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1824:
RiskId: 431
ComplianceId: 443
RiskTitle: Non-compliance with Regulatory Requirements
Criticality: High
PossibleDamage: Legal actions, financial penalties, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Direct impact on compliance operations and legal standing
RiskDescription: Failure to comply with regulatory requirements related to climate change could result
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for compliance staff", "2": "Engage external consultants for regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1825:
RiskId: 432
ComplianceId: 444
RiskTitle: Inadequate Audit Documentation
Criticality: Medium
PossibleDamage: Legal non-compliance, regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Direct impact on compliance audit processes and legal standing
RiskDescription: Inadequate audit documentation could lead to legal challenges, regulatory fines, and
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement robust audit trail systems", "2": "Regularly review audit documentation
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1826:
RiskId: 433
ComplianceId: 445
RiskTitle: Climate-Related Risk Exposure
Criticality: High
PossibleDamage: Financial losses and reputational damage due to inadequate risk mitigation
Category: Environmental
RiskType: Residual
BusinessImpact: Potential disruptions to operations and negative impact on brand reputation
RiskDescription: Failure to effectively mitigate climate-related risks may result in increased vulnerability

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement risk transfer options", "2": "Enhance monitoring and reporting mechani
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1827:
RiskId: 434
ComplianceId: 446
RiskTitle: Failure to Integrate Climate-Related Risks into Overall Risk Management Framework
Criticality: High
PossibleDamage: Increased exposure to climate-related risks, financial losses, reputational damage, r
Category: Environmental
RiskType: Residual
BusinessImpact: All business units may be impacted by climate-related risks
RiskDescription: Failure to integrate climate-related risks into the overall risk management framework r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on climate-related risks", "2": "Integrati
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1828:
RiskId: 435

ComplianceId: 447
RiskTitle: Inaccurate GHG Emissions Reporting
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of stakeholder trust
Category: Environmental
RiskType: Current
BusinessImpact: Loss of credibility, regulatory scrutiny, financial penalties
RiskDescription: Failure to accurately report GHG emissions may lead to legal and financial consequer
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GHG calculation methodologies", "2": "Internal audits to verify
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1829:
RiskId: 436
ComplianceId: 448
RiskTitle: Misalignment of Climate-related Metrics
Criticality: High
PossibleDamage: Misalignment may lead to reputational damage, decreased employee morale, and p
Category: Operational
RiskType: Current
BusinessImpact: Potential decrease in organizational performance and stakeholder trust.
RiskDescription: Failure to integrate climate-related metrics in performance evaluations may result in m
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting of climate-related metrics integration", "2": "Eng
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1830:
RiskId: 437
ComplianceId: 449
RiskTitle: Inaccurate Scope 3 GHG Emissions Disclosure
Criticality: High
PossibleDamage: Reputational damage, financial penalties, loss of investor trust
Category: Environmental
RiskType: Current
BusinessImpact: Potential loss of clients, decreased investment opportunities, regulatory fines
RiskDescription: Failure to accurately disclose Scope 3 GHG emissions can lead to reputational dama
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training sessions for the sustainability reporting team on GHG
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1831:
RiskId: 438
ComplianceId: 450
RiskTitle: Inaccurate Reporting of WACI
Criticality: High
PossibleDamage: Misleading sustainability reports and reputational damage

Category: Operational
RiskType: Current
BusinessImpact: Negative impact on investment decisions and client relationships
RiskDescription: Failure to accurately report WACI may lead to incorrect assessment of carbon footprin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for accurate WACI calculation", "2": "Implement automa
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1832:
RiskId: 439
ComplianceId: 451
RiskTitle: Non-compliance with Climate-related Targets Disclosure
Criticality: High
PossibleDamage: Loss of credibility, regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Loss of stakeholder trust, financial penalties
RiskDescription: Failure to disclose accurate climate-related targets can lead to regulatory fines, reputa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting of targets", "2": "Engagement with stakeholders
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1833:
RiskId: 440
ComplianceId: 452
RiskTitle: Inadequate Governance of Climate-Related Risks
Criticality: High
PossibleDamage: Financial losses, regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Financial instability, loss of investor confidence, regulatory scrutiny
RiskDescription: Failure to establish a climate risk committee may result in inadequate oversight of clim
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a dedicated climate risk committee", "2": "Provide training on climate ris
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1834:
RiskId: 441
ComplianceId: 453
RiskTitle: Inaccurate Total Carbon Emissions Reporting
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor confidence
Category: Environmental
RiskType: Current
BusinessImpact: Potential loss of credibility and trust from stakeholders
RiskDescription: Failure to accurately report total carbon emissions can lead to misinformed decisions

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular audits to ensure accuracy of calculations", "2": "Provide trainin
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1835:
RiskId: 442
ComplianceId: 454
RiskTitle: Inaccurate Weighted Average Carbon Intensity Reporting
Criticality: Medium
PossibleDamage: Misrepresentation of environmental impact, regulatory scrutiny
Category: Environmental
RiskType: Current
BusinessImpact: Potential regulatory fines and reputational damage
RiskDescription: Misreporting weighted average carbon intensity can lead to inaccurate assessment of
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement standardized methodologies for consistent calculations", "2": "Regularl
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1836:
RiskId: 443

ComplianceId: 455
RiskTitle: Inaccurate Calculation of Carbon Emissions
Criticality: High
PossibleDamage: Misleading sustainability reports, Regulatory fines
Category: Environmental
RiskType: Current
BusinessImpact: Potential reputational damage, Legal implications
RiskDescription: Incorrect calculation of carbon emissions can lead to misinformed decision-making ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training sessions for portfolio managers and sustainability offic
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1837:
RiskId: 444
ComplianceId: 456
RiskTitle: Non-Compliance with Annual Reporting of Carbon Emissions
Criticality: Medium
PossibleDamage: Regulatory fines, Reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial penalties, Loss of investor trust
RiskDescription: Failure to report annual carbon emissions accurately can result in regulatory fines and
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish a dedicated reporting process for annual carbon emissions", "2": "Condu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1838:
RiskId: 445
ComplianceId: 457
RiskTitle: Inaccurate Carbon Intensity Reporting
Criticality: High
PossibleDamage: Misinformed investment decisions and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Negative impact on investment decisions and stakeholder trust
RiskDescription: Incorrect carbon intensity calculations may lead to misinformed investment decisions
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on calculation methodology", "2": "Automated tools for data colle
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1839:
RiskId: 446
ComplianceId: 458
RiskTitle: Failure to Report Annual Carbon Intensity
Criticality: Medium
PossibleDamage: Regulatory non-compliance penalties and loss of investor trust

Category: Operational
RiskType: Current
BusinessImpact: Financial penalties and reputational damage
RiskDescription: Failure to report annual carbon intensity may lead to regulatory penalties and loss of i
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting timelines and responsibilities", "2": "Internal reviews of re
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1840:
RiskId: 447
ComplianceId: 459
RiskTitle: Inaccurate Calculation of Carbon-Related Assets
Criticality: High
PossibleDamage: Misleading stakeholders, potential regulatory fines
Category: Compliance
RiskType: Current
BusinessImpact: Financial reporting and stakeholder trust
RiskDescription: Incorrect calculation of carbon-related assets leading to inaccurate disclosure and pot
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular audits to verify accuracy of calculations", "2": "Provide training
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1841:
RiskId: 448
ComplianceId: 460
RiskTitle: Missed Annual Disclosure Deadline
Criticality: Medium
PossibleDamage: Non-compliance penalties, loss of stakeholder trust
Category: Compliance
RiskType: Current
BusinessImpact: Financial reporting and stakeholder trust
RiskDescription: Failure to disclose carbon-related assets annually leading to penalties and negative p
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a calendar reminder system for disclosure deadlines", "2": "Establish c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1842:
RiskId: 449
ComplianceId: 461
RiskTitle: Lack of Timely Reporting on Climate-related Risks and Opportunities
Criticality: High
PossibleDamage: Uninformed decision-making, missed opportunities for risk mitigation and strategic p
Category: Operational
RiskType: Inherent
BusinessImpact: Compromised board oversight and decision-making processes
RiskDescription: Failure to provide timely updates on climate-related risks and opportunities may lead t

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting timelines and expectations", "2": "Implement automated
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1843:
RiskId: 450
ComplianceId: 462
RiskTitle: Failure to Conduct Bi-annual Climate-related Risk Assessment
Criticality: High
PossibleDamage: Inadequate risk management and missed opportunities for the organization
Category: Environmental
RiskType: Inherent
BusinessImpact: All business units may be impacted by climate-related risks
RiskDescription: Failure to conduct bi-annual assessments may lead to a lack of awareness and prepa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication and accountability for assessment timelines", "2": "P
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1844:
RiskId: 451

ComplianceId: 463
RiskTitle: Missed Opportunities for Strategic Planning
Criticality: High
PossibleDamage: Failure to identify opportunities may result in competitive disadvantage and loss of m
Category: Strategic
RiskType: Inherent
BusinessImpact: Loss of market share, decreased revenue, and diminished brand value.
RiskDescription: Failure to identify and capitalize on climate-related opportunities may hinder the orgar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a dedicated team to monitor and evaluate emerging opportunities", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1845:
RiskId: 452
ComplianceId: 464
RiskTitle: Inaccurate Financial Forecasts due to Climate-Related Risks
Criticality: High
PossibleDamage: Financial losses, misallocation of capital
Category: Financial
RiskType: Inherent
BusinessImpact: Potential impact on financial performance and strategic decision-making
RiskDescription: Failure to integrate climate-related risks could lead to inaccurate financial forecasts, m
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training on climate scenarios and financial impact assessment", "2": "Eng
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1846:
RiskId: 453
ComplianceId: 465
RiskTitle: Failure to Meet GHG Emissions Reduction Targets
Criticality: High
PossibleDamage: Increased carbon footprint, regulatory fines, reputational damage
Category: Environmental
RiskType: Current
BusinessImpact: Potential increase in operational costs, loss of competitive advantage
RiskDescription: Not achieving set GHG emissions reduction targets may lead to negative environmen
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implementing energy-efficient practices", "2": "Investing in renewable energy sour
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1847:
RiskId: 454
ComplianceId: 466
RiskTitle: Inadequate Progress Tracking towards GHG Emissions Reduction Targets
Criticality: Medium
PossibleDamage: Deviation from targets, missed opportunities for improvement

Category: Environmental
RiskType: Current
BusinessImpact: Potential delay in achieving emissions reduction goals
RiskDescription: Lack of regular progress tracking may result in inefficiencies and hinder the organizati
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing automated tracking systems", "2": "Enhancing communication chan
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1848:
RiskId: 455
ComplianceId: 467
RiskTitle: Financial Losses from Climate-Related Events
Criticality: High
PossibleDamage: Financial losses due to inadequate resilience planning
Category: Financial
RiskType: Inherent
BusinessImpact: All business units within the organization
RiskDescription: Failure to conduct scenario analysis may lead to unanticipated financial losses from c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for Risk Management Team and Financial Analysts on scenario a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1849:
RiskId: 456
ComplianceId: 468
RiskTitle: Climate Risk Exposure
Criticality: High
PossibleDamage: Financial losses, reputational damage, and regulatory penalties
Category: Environmental
RiskType: Inherent
BusinessImpact: Potential disruptions to operations, supply chain issues, and legal liabilities
RiskDescription: Climate-related risks pose a significant threat to the organization's operations and fina
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement climate risk monitoring and early warning systems", "2": "Diversify sup
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1850:
RiskId: 457
ComplianceId: 469
RiskTitle: Failure to Conduct Annual Climate Risk Assessment
Criticality: High
PossibleDamage: Increased vulnerability to climate-related risks and potential financial losses
Category: Environmental
RiskType: Inherent
BusinessImpact: Financial losses, reputational damage, and operational disruptions
RiskDescription: Failure to conduct annual climate risk assessments may result in the organization bei

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust risk assessment process", "2": "Engage relevant department
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1851:
RiskId: 458
ComplianceId: 470
RiskTitle: Financial Losses from Unmitigated Climate Risks
Criticality: High
PossibleDamage: Significant financial losses due to unanticipated climate-related events
Category: Operational
RiskType: Inherent
BusinessImpact: Financial impact on revenue and profitability
RiskDescription: Failure to integrate climate risks may result in unforeseen financial losses from extrem
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update risk management strategies to reflect climate-related risks and c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1852:
RiskId: 459

ComplianceId: 471
RiskTitle: Inaccurate Assessment of Climate Risks
Criticality: High
PossibleDamage: Inadequate risk management, regulatory non-compliance
Category: Environmental
RiskType: Current
BusinessImpact: Potential fines, reputational damage
RiskDescription: Failure to establish accurate metrics and targets may lead to misinformed decisions a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review of metrics and targets", "2": "Engagement with industry peers for b
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1853:
RiskId: 460
ComplianceId: 472
RiskTitle: Inefficient Resource Allocation
Criticality: High
PossibleDamage: Lack of clear targets may lead to inefficient resource allocation and missed sustaina
Category: Environmental
RiskType: Current
BusinessImpact: Resource wastage, missed sustainability goals
RiskDescription: Failure to define clear targets annually may result in misalignment of resources and m
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training and guidance on target setting", "2": "Regular monitoring and rep

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 1854:

RiskId: 461

ComplianceId: 473

RiskTitle: Inaccurate Reporting

Criticality: Medium

PossibleDamage: Outdated methodologies may lead to inaccurate target setting and reporting

Category: Environmental

RiskType: Current

BusinessImpact: Misleading stakeholders, regulatory fines

RiskDescription: Failure to review methodologies every two years may result in inaccurate reporting of

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regular review and update of methodologies", "2": "External audit of methodologi

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 1855:

RiskId: 462

ComplianceId: 474

RiskTitle: Misalignment of Targets with Stakeholder Expectations

Criticality: High

PossibleDamage: Reputational damage, decreased investor confidence, and community trust

Category: Reputational
RiskType: Current
BusinessImpact: All business units within the organization
RiskDescription: Failure to engage stakeholders may result in setting targets that do not reflect stakeho
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular stakeholder engagement sessions", "2": "Transparent communication on
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1856:
RiskId: 463
ComplianceId: 475
RiskTitle: Limited Stakeholder Input on Climate-Related Targets
Criticality: Medium
PossibleDamage: Decreased credibility and trust, narrow perspectives on targets
Category: Reputational
RiskType: Current
BusinessImpact: Investor Relations and Sustainability teams
RiskDescription: Limited stakeholder input may result in setting targets that do not reflect the diverse p
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Ensure diverse representation in engagement activities", "2": "Analyze and incorp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1857:
RiskId: 464
ComplianceId: 476
RiskTitle: Inaccurate Water Stress Metrics Reporting
Criticality: High
PossibleDamage: Inaccurate reporting may lead to stakeholder distrust and regulatory non-compliance
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential fines, reputational damage, and loss of stakeholder confidence.
RiskDescription: Failure to accurately report water stress metrics can result in misleading information b
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training for data collection and reporting teams", "2": "Conduct
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1858:
RiskId: 465
ComplianceId: 477
RiskTitle: Inaccurate Scope 1 Emissions Reporting
Criticality: High
PossibleDamage: Fines, reputational damage, legal action
Category: Environmental
RiskType: Current
BusinessImpact: Financial penalties, loss of trust from stakeholders
RiskDescription: Failure to accurately report Scope 1 emissions can lead to regulatory non-compliance

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for the environmental compliance team on emissions tracking", "2
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1859:
RiskId: 466
ComplianceId: 478
RiskTitle: Lack of External Verification for Scope 1 Emissions
Criticality: Medium
PossibleDamage: Credibility issues, lack of trust from stakeholders
Category: Environmental
RiskType: Current
BusinessImpact: Loss of credibility, decreased stakeholder trust
RiskDescription: Failure to have external verification of Scope 1 emissions may raise doubts about the
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Engage reputable external auditors for emissions verification", "2": "Implement rol
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1860:
RiskId: 467

ComplianceId: 479
RiskTitle: Non-compliance with Energy Efficiency Metrics Disclosure
Criticality: High
PossibleDamage: Loss of credibility, regulatory fines, and reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential financial losses and damage to organizational reputation
RiskDescription: Failure to disclose accurate energy efficiency metrics can result in regulatory non-com
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data verification processes", "2": "Engage with regulators to ens
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1861:
RiskId: 468
ComplianceId: 480
RiskTitle: Misalignment between Energy Efficiency Metrics and Sustainability Reporting
Criticality: Medium
PossibleDamage: Confusion among stakeholders and investors, inconsistency in organizational messa
Category: Operational
RiskType: Current
BusinessImpact: Potential confusion among stakeholders and investors, impacting organizational cred
RiskDescription: Misalignment between energy efficiency metrics and sustainability reporting can lead
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish clear reporting guidelines for alignment", "2": "Provide training on sustai

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 1862:

RiskId: 469

ComplianceId: 481

RiskTitle: Inaccurate Reporting of GHG Emissions and Water Usage Data

Criticality: High

PossibleDamage: Regulatory fines, reputational damage, loss of stakeholder trust

Category: Environmental

RiskType: Current

BusinessImpact: Potential financial losses and damage to organizational reputation

RiskDescription: Failure to accurately report GHG emissions and water usage data may lead to regulat

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 72

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement robust data verification processes", "2": "Conduct regular internal audit

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1863:

RiskId: 470

ComplianceId: 482

RiskTitle: Failure to Implement Waste Reduction Initiatives

Criticality: High

PossibleDamage: Increased waste generation, higher disposal costs, negative environmental impact

Category: Environmental
RiskType: Inherent
BusinessImpact: All business units would be impacted by increased waste generation and disposal cos
RiskDescription: Failure to implement waste reduction initiatives may lead to higher waste generation,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for employees on waste management practices", "2": "E
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1864:
RiskId: 471
ComplianceId: 483
RiskTitle: Failure to Conduct Semi-Annual Waste Audits
Criticality: Medium
PossibleDamage: Inaccurate waste data, ineffective recycling programs, missed opportunities for impr
Category: Environmental
RiskType: Inherent
BusinessImpact: Environmental department would be impacted by inaccurate waste data and ineffectiv
RiskDescription: Failure to conduct semi-annual waste audits may lead to inaccurate waste data, ineffe
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear audit procedures and checklists", "2": "Provide training to the Envi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 1865:
RiskId: 472
ComplianceId: 484
RiskTitle: Inadequate Climate-Related Disclosures
Criticality: High
PossibleDamage: Misleading stakeholders and investors, potential financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Reputational damage, financial losses
RiskDescription: Failure to provide relevant and material climate-related disclosures may result in stake
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear criteria for assessing materiality and relevance", "2": "Seek feedba
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1866:
RiskId: 473
ComplianceId: 485
RiskTitle: Inaccurate Climate-Related Disclosures
Criticality: High
PossibleDamage: Regulatory fines, loss of stakeholder trust, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential financial losses and damage to organizational reputation
RiskDescription: Failure to provide accurate and comprehensive climate-related disclosures could resu

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on reporting requirements", "2": "Internal audits for accuracy che
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1867:
RiskId: 474
ComplianceId: 486
RiskTitle: Misinterpretation of Financial Information
Criticality: High
PossibleDamage: Loss of investor trust, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Could lead to financial losses and reputational damage
RiskDescription: Failure to communicate financial information clearly could result in stakeholders misu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training on clear communication practices", "2": "Use plain language guid
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1868:
RiskId: 475

ComplianceId: 487
RiskTitle: Misinterpretation of Climate-Related Data
Criticality: High
PossibleDamage: Loss of investor trust and potential divestment
Category: Operational
RiskType: Current
BusinessImpact: Financial losses and reputational damage
RiskDescription: Inconsistencies in reporting formats may lead to misinterpretation of climate-related d
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on standardized reporting formats", "2": "Automated val
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1869:
RiskId: 476
ComplianceId: 488
RiskTitle: Misalignment with Industry Standards
Criticality: High
PossibleDamage: Loss of credibility and trust from stakeholders
Category: Operational
RiskType: Residual
BusinessImpact: Direct impact on financial decision-making and stakeholder relationships.
RiskDescription: Failure to align with industry standards may result in inaccurate benchmarking and as
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regular training on industry standards for finance and strategy teams", "2": "Interr

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 1870:

RiskId: 477

ComplianceId: 489

RiskTitle: Data Collection Delay Risk

Criticality: Medium

PossibleDamage: Delayed or inaccurate data collection leading to unreliable climate-related disclosure

Category: Operational

RiskType: Current

BusinessImpact: Sustainability reporting credibility and regulatory penalties

RiskDescription: Risk of delayed or inaccurate data collection impacting the reliability of climate-related

RiskLikelihood: 6

RiskImpact: 8

RiskExposureRating: 48

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regular training on data collection procedures", "2": "Automated data collection to

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 1871:

RiskId: 478

ComplianceId: 490

RiskTitle: Data Verification Failure Risk

Criticality: High

PossibleDamage: Inaccurate or unreliable climate-related data in disclosures

Category: Operational
RiskType: Current
BusinessImpact: Regulatory fines, loss of stakeholder trust
RiskDescription: Risk of inaccurate or unreliable climate-related data in disclosures due to failed verific
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Independent verification by third-party auditors", "2": "Regular review of verificatio
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1872:
RiskId: 479
ComplianceId: 491
RiskTitle: Inaccurate Climate Disclosures
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, non-compliance penalties
Category: Compliance
RiskType: Inherent
BusinessImpact: Loss of stakeholder trust, financial penalties, legal consequences
RiskDescription: Failure to establish a governance framework for climate disclosures may result in inac
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for relevant personnel on governance framework requir
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1873:
RiskId: 480
ComplianceId: 492
RiskTitle: Failure to Adhere to Reporting Schedule
Criticality: High
PossibleDamage: Inaccurate or delayed climate-related disclosures, reputational damage, regulatory n
Category: Operational
RiskType: Current
BusinessImpact: May impact the organization's reputation, regulatory standing, and stakeholder trust
RiskDescription: Failure to adhere to the reporting schedule may result in inaccurate or delayed climate
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of reporting deadlines", "2": "Training for reporting team on sc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1874:
RiskId: 481
ComplianceId: 493
RiskTitle: Inadequate Crisis Communication
Criticality: High
PossibleDamage: Loss of stakeholder trust, reputational damage, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: All business units involved in climate-related reporting
RiskDescription: Failure to communicate effectively during crisis events can lead to severe consequen

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication protocols and roles", "2": "Regular training and dril
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1875:
RiskId: 482
ComplianceId: 494
RiskTitle: Inaccurate Financial Reporting
Criticality: High
PossibleDamage: Financial losses, regulatory penalties, investor distrust
Category: Operational
RiskType: Current
BusinessImpact: Impact on financial statements, compliance requirements
RiskDescription: Failure to assess transition risks annually may lead to inaccurate financial reporting, r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust risk assessment frameworks and tools", "2": "Regularly update
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1876:
RiskId: 483

ComplianceId: 495
RiskTitle: Misinformation in Financial Reports
Criticality: Medium
PossibleDamage: Loss of stakeholder trust, regulatory fines, reputational harm
Category: Financial
RiskType: Current
BusinessImpact: Stakeholder confidence, regulatory compliance
RiskDescription: Failure to disclose transition risks in financial reports may result in misinformation, lea
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting guidelines for transition risks", "2": "Conduct regular audi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1877:
RiskId: 484
ComplianceId: 496
RiskTitle: Increased Frequency of Extreme Weather Events
Criticality: High
PossibleDamage: Operational disruptions and financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: Potential interruptions to operations and financial performance
RiskDescription: The risk of increased frequency of extreme weather events may lead to disruptions in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Develop contingency plans for extreme weather events", "2": "Invest in infrastruct
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1878:
RiskId: 485
ComplianceId: 497
RiskTitle: Missed Climate-Related Opportunities
Criticality: High
PossibleDamage: Financial loss and decreased organizational resilience
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to identify and capitalize on climate-related opportunities can result in missed
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for employees on identifying opportuni
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1879:
RiskId: 486
ComplianceId: 498
RiskTitle: Revenue Impact Assessment Failure
Criticality: High
PossibleDamage: Loss of market share, decreased revenue, missed growth opportunities

Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, decreased competitiveness
RiskDescription: Failure to assess revenue impact could result in missed growth opportunities, decreas
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement proactive market monitoring", "2": "Develop contingency plans for reve
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1880:
RiskId: 487
ComplianceId: 499
RiskTitle: Failure to Evaluate Operating Expenditures Annually
Criticality: High
PossibleDamage: Increased operating costs, missed efficiency improvements, regulatory non-compliar
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, decreased operational efficiency, reputational damage
RiskDescription: Not conducting the annual evaluation of operating expenditures may lead to unforese
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust data analysis process to accurately project future costs based
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1881:
RiskId: 488
ComplianceId: 500
RiskTitle: Investment Vulnerability to Climate Risks
Criticality: High
PossibleDamage: Financial losses and reputational damage due to climate risk exposure
Category: Financial
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to align capital expenditures with climate risk mitigation strategies may result i
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular climate risk assessments for all capital projects", "2": "Diversification of in
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1882:
RiskId: 489
ComplianceId: 501
RiskTitle: Inaccurate Asset Valuations
Criticality: High
PossibleDamage: Financial losses, regulatory penalties, reputational damage
Category: Financial
RiskType: Inherent
BusinessImpact: Potential write-offs, misrepresentation of financial health
RiskDescription: Failure to accurately assess the impact of climate-related risks on asset valuations ma

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training on climate risk factors for asset valuation teams", "2": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1883:
RiskId: 490
ComplianceId: 502
RiskTitle: Inaccurate Assessment of Climate Risks on Debt Liabilities
Criticality: High
PossibleDamage: Misleading financial disclosures, increased debt burden, reduced creditworthiness
Category: Financial
RiskType: Inherent
BusinessImpact: Financial mismanagement, reduced investor confidence
RiskDescription: Failure to accurately assess climate risks could lead to misinformed financial decision
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on climate risk assessment", "2": "Engage external experts for sp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1884:
RiskId: 491

ComplianceId: 503
RiskTitle: Misrepresentation of Equity Capital Costs
Criticality: High
PossibleDamage: Loss of investor trust, legal consequences
Category: Financial
RiskType: Current
BusinessImpact: Financial losses, reputational damage
RiskDescription: Failure to accurately assess and report equity capital costs in relation to climate risks
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on climate risk analysis", "2": "Clear reporting guidelines", "3": "A
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1885:
RiskId: 492
ComplianceId: 504
RiskTitle: Asset Vulnerability to Transition and Physical Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage, and regulatory penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Potential disruptions to operations, supply chains, and financial performance
RiskDescription: Assets exposed to transition and physical risks may face devaluation, operational disr
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement risk management strategies", "2": "Enhance climate risk monitoring", "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1886:
RiskId: 493
ComplianceId: 505
RiskTitle: Misrepresentation of Capital Deployment Data
Criticality: High
PossibleDamage: Financial penalties, loss of investor trust, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Potential impact on financial reporting accuracy and investor confidence
RiskDescription: Failure to accurately report capital deployment for climate initiatives may lead to misin
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular data validation checks", "2": "Internal controls for accurate reporting", "3"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1887:
RiskId: 494
ComplianceId: 506
RiskTitle: Inaccurate Reporting of GHG Emissions
Criticality: High
PossibleDamage: Legal fines, reputational damage, loss of investor confidence

Category: Environmental
RiskType: Current
BusinessImpact: Financial losses, regulatory non-compliance, negative stakeholder perception
RiskDescription: Failure to accurately report Scope 1 and Scope 2 GHG emissions may lead to legal re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data verification processes", "2": "Engage external auditors for i
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1888:
RiskId: 495
ComplianceId: 507
RiskTitle: Inaccurate Scope 3 Emissions Disclosure
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of stakeholder trust
Category: Environmental
RiskType: Current
BusinessImpact: Financial penalties, decreased investor confidence, negative public perception
RiskDescription: Failure to accurately disclose Scope 3 emissions can result in legal and financial cons
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data verification processes", "2": "Engage with external auditors
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1889:
RiskId: 496
ComplianceId: 508
RiskTitle: Inaccurate Climate Risk Disclosure
Criticality: High
PossibleDamage: Loss of investor trust, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial performance, stakeholder trust, regulatory standing
RiskDescription: Failure to provide accurate and comprehensive climate risk disclosures can lead to fi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust risk assessment processes", "2": "Engage with climate risk exp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1890:
RiskId: 497
ComplianceId: 509
RiskTitle: Misalignment of Executive Remuneration with Sustainability Objectives
Criticality: High
PossibleDamage: Decreased motivation, performance issues, and retention challenges among executi
Category: Operational
RiskType: Current
BusinessImpact: Potential decrease in organizational performance and sustainability efforts
RiskDescription: Failure to integrate climate metrics in executive remuneration may lead to executives

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular communication on the importance of climate metrics in remuneration", "2
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1891:
RiskId: 498
ComplianceId: 510
RiskTitle: Unidentified Climate Risk Impact
Criticality: High
PossibleDamage: Financial losses due to unidentified climate risks impacting operations
Category: Operational
RiskType: Inherent
BusinessImpact: All operational units
RiskDescription: Failure to identify and assess climate-related risks may result in operational disruptior
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement risk management strategies based on assessment findings", "2": "Reg
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1892:
RiskId: 499

ComplianceId: 511
RiskTitle: Inaccurate Climate Risk Reporting
Criticality: High
PossibleDamage: Loss of stakeholder trust, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory fines, reputational damage
RiskDescription: Failure to accurately report climate risks could lead to incorrect decision-making and p
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on climate risk reporting for all departments", "2": "Continuous m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1893:
RiskId: 500
ComplianceId: 512
RiskTitle: Misalignment of Governance Structure
Criticality: High
PossibleDamage: Loss of stakeholder trust, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: All business units could be impacted by ineffective governance structure
RiskDescription: Failure to disclose accurate governance structure could lead to misinformed stakehol
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular review and update of governance structure", "2": "Engagement with stake
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1894:
RiskId: 501
ComplianceId: 513
RiskTitle: Inaccurate Disclosure of Risk Management Processes
Criticality: High
PossibleDamage: Loss of stakeholder trust, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation, legal consequences
RiskDescription: Failure to accurately disclose risk management processes in annual financial filings c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of risk disclosures", "2": "Internal and external audits c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1895:
RiskId: 502
ComplianceId: 514
RiskTitle: Failure to Meet GHG Emissions Reduction Targets
Criticality: High
PossibleDamage: Missed emissions reduction targets, reputational damage

Category: Environmental
RiskType: Current
BusinessImpact: Loss of credibility, regulatory fines, increased operational costs
RiskDescription: Failure to achieve the set greenhouse gas emissions reduction targets may lead to re
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting on progress towards targets", "2": "Engagement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1896:
RiskId: 503
ComplianceId: 515
RiskTitle: Missed Annual Value Chain Assessment
Criticality: High
PossibleDamage: Missed opportunities for emissions reduction and sustainability improvements.
Category: Environmental
RiskType: Residual
BusinessImpact: Negative impact on sustainability goals and reputational damage.
RiskDescription: Failure to conduct the annual review may result in missed opportunities for emissions
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a regular monitoring system to track changes in operations and extern
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1897:
RiskId: 504
ComplianceId: 516
RiskTitle: Failure to Assess Climate-Related Risks
Criticality: High
PossibleDamage: Inadequate risk management and missed opportunities for mitigating climate-related
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, reputational damage, regulatory non-compliance
RiskDescription: Failure to assess climate-related risks annually may result in the organization being u
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training for Risk Management Department on climate-related ri
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1898:
RiskId: 505
ComplianceId: 517
RiskTitle: Inadequate Oversight of Climate-related Disclosures
Criticality: High
PossibleDamage: Misinformation, non-compliance with regulatory requirements, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Potential regulatory fines, reputational damage, legal actions
RiskDescription: Failure to establish the Climate Risk Oversight Committee may result in inadequate o

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for committee members", "2": "Establis
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1899:
RiskId: 506
ComplianceId: 518
RiskTitle: Inaccurate Climate-Related Financial Disclosures
Criticality: High
PossibleDamage: Loss of investor trust, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: Financial and reputational damage
RiskDescription: Incorrect or delayed disclosures may lead to misinformed investment decisions and le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust review processes for disclosures", "2": "Engage external audito
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1900:
RiskId: 507

ComplianceId: 519
RiskTitle: Failure to Conduct Annual Climate-Related Risk Assessment
Criticality: High
PossibleDamage: Inadequate risk management and missed opportunities for mitigating climate-related
Category: Environmental
RiskType: Inherent
BusinessImpact: All business units may be impacted by climate-related risks
RiskDescription: Failure to conduct the annual risk assessment may lead to increased exposure to clim
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely completion of the assessment", "2": "Regularly review and update r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1901:
RiskId: 508
ComplianceId: 520
RiskTitle: Misleading Financial Disclosures
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor trust
Category: Compliance
RiskType: Current
BusinessImpact: Negative impact on financial performance, legal implications, and stakeholder relation
RiskDescription: Failure to comply with disclosure requirements may lead to inaccurate or incomplete f
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training on disclosure requirements", "2": "Internal audits to ensure accur
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1902:
RiskId: 509
ComplianceId: 521
RiskTitle: Unidentified Climate Risk Impact
Criticality: High
PossibleDamage: Financial losses due to unidentified climate-related risks
Category: Financial
RiskType: Inherent
BusinessImpact: Risk management, asset management
RiskDescription: Failure to identify and assess climate-related risks may lead to financial losses and as
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on climate risk assessment techniques", "2": "Utilize external exp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1903:
RiskId: 510
ComplianceId: 522
RiskTitle: Inaccurate Climate Risk Disclosure
Criticality: High
PossibleDamage: Loss of stakeholder trust, regulatory fines

Category: Compliance
RiskType: Current
BusinessImpact: Negative impact on reputation and financial performance
RiskDescription: Failure to accurately report climate-related risks as per TCFD guidelines
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on TCFD guidelines", "2": "Internal audits to ensure compliance",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1904:
RiskId: 511
ComplianceId: 523
RiskTitle: Financial Impact of Market Shifts
Criticality: High
PossibleDamage: Significant financial losses due to sudden market changes
Category: Operational
RiskType: Inherent
BusinessImpact: Could affect revenue streams and profitability
RiskDescription: Market shifts towards low-carbon technologies could render current products/services
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Diversify product/service offerings", "2": "Monitor market trends closely", "3": "Dev
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1905:
RiskId: 512
ComplianceId: 524
RiskTitle: Non-Compliance with Climate Disclosure Requirements
Criticality: High
PossibleDamage: Loss of stakeholder trust, regulatory fines, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial penalties, legal actions, reputational damage
RiskDescription: Failure to comply with climate disclosure requirements can result in inaccurate inform
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on disclosure requirements", "2": "Internal audits to ensure comp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 1906:
RiskId: 513
ComplianceId: 525
RiskTitle: Ineffective Stakeholder Engagement
Criticality: High
PossibleDamage: Loss of stakeholder trust, reputational damage
Category: Reputational
RiskType: Inherent
BusinessImpact: Direct impact on corporate reputation and relationships with stakeholders
RiskDescription: Failure to engage stakeholders effectively could result in negative perceptions, lack o

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for staff involved in stakeholder engagement", "2": "Continuous m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1907:
RiskId: 514
ComplianceId: 526
RiskTitle: Inaccurate Fleet Fuel Economy Reporting
Criticality: High
PossibleDamage: Non-compliance penalties, reputational damage, loss of investor confidence
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, regulatory fines, damage to brand reputation
RiskDescription: Failure to accurately report fleet fuel economy data may result in regulatory penalties,
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular data quality checks", "2": "Provide training on accurate data co
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1908:
RiskId: 515

ComplianceId: 527
RiskTitle: Non-Disclosure of EEDI Metrics in Financial Reports
Criticality: Medium
PossibleDamage: Non-compliance penalties, investor mistrust, regulatory scrutiny
Category: Financial
RiskType: Current
BusinessImpact: Financial losses, reputational damage, regulatory fines
RiskDescription: Failure to integrate EEDI reporting in financial disclosures may result in non-complian
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting guidelines", "2": "Conduct regular audits of financial disc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1909:
RiskId: 516
ComplianceId: 528
RiskTitle: Failure to Identify Regulatory Changes
Criticality: High
PossibleDamage: Financial losses due to non-compliance penalties
Category: Financial
RiskType: Inherent
BusinessImpact: Potential fines and reputational damage
RiskDescription: Failure to identify regulatory changes could result in non-compliance penalties and fin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly monitor regulatory updates", "2": "Engage legal counsel for compliance
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1910:
RiskId: 517
ComplianceId: 529
RiskTitle: Inaccurate Greenhouse Gas Emissions Reporting
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, stakeholder distrust
Category: Environmental
RiskType: Current
BusinessImpact: Financial penalties, reputational damage, loss of stakeholder trust
RiskDescription: Failure to report accurate greenhouse gas emissions data could result in regulatory n
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular data quality checks", "2": "Provide training to staff on data colle
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1911:
RiskId: 518
ComplianceId: 530
RiskTitle: Missed Energy Consumption Metrics Updates
Criticality: Medium
PossibleDamage: Missed energy efficiency targets, increased energy costs, stakeholder dissatisfactio

Category: Operational
RiskType: Current
BusinessImpact: Increased energy costs, missed efficiency targets, stakeholder dissatisfaction
RiskDescription: Failure to provide timely updates on energy consumption metrics could result in misse
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels for progress updates", "2": "Implement e
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1912:
RiskId: 519
ComplianceId: 531
RiskTitle: Failure to Conduct Annual Water Usage Assessment
Criticality: High
PossibleDamage: Increased water costs, reputational damage, and regulatory fines
Category: Environmental
RiskType: Current
BusinessImpact: Potential operational disruptions and financial losses
RiskDescription: Not conducting the annual water usage assessment could result in inefficient water m
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement water management tools", "2": "Train staff on water conservation pract
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1913:
RiskId: 520
ComplianceId: 532
RiskTitle: Failure to Implement Ongoing Water Usage Monitoring
Criticality: Medium
PossibleDamage: Inefficiencies, increased costs, and environmental impact
Category: Environmental
RiskType: Current
BusinessImpact: Operational disruptions and financial losses
RiskDescription: Not monitoring water usage continuously could lead to missed conservation opportun
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review water usage data", "2": "Implement real-time monitoring systems
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1914:
RiskId: 521
ComplianceId: 533
RiskTitle: Failure to Disclose R&DDD Initiatives
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of investor confidence
Category: Compliance
RiskType: Current
BusinessImpact: Negative impact on sustainability goals and stakeholder trust
RiskDescription: Non-disclosure of R&DDD initiatives can lead to regulatory non-compliance and dama

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear documentation and reporting processes", "2": "Implement regular i
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1915:
RiskId: 522
ComplianceId: 534
RiskTitle: Increased Carbon Footprint
Criticality: High
PossibleDamage: Environmental impact and regulatory fines
Category: Environmental
RiskType: Current
BusinessImpact: Increased operational costs and reputational damage
RiskDescription: Failure to reduce GHG emissions may lead to negative environmental consequences
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting of emissions data", "2": "Implementation of ener
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1916:
RiskId: 523

ComplianceId: 535
RiskTitle: Outdated Emissions Reduction Plan
Criticality: Medium
PossibleDamage: Missed targets and ineffective emissions reduction efforts
Category: Environmental
RiskType: Current
BusinessImpact: Ineffective sustainability efforts and potential regulatory non-compliance
RiskDescription: An outdated emissions reduction plan may not align with current goals and practices,
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update meetings with stakeholders", "2": "Utilization of update
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1917:
RiskId: 524
ComplianceId: 536
RiskTitle: Inefficient Water Usage
Criticality: Medium
PossibleDamage: Increased costs and environmental impact
Category: Environmental
RiskType: Current
BusinessImpact: Higher operational costs and potential regulatory fines
RiskDescription: Failure to conduct biannual water usage assessments may result in excessive water c
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement water-saving technologies", "2": "Train staff on water conservation pra

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 1918:

RiskId: 525

ComplianceId: 537

RiskTitle: Lack of Conservation Documentation

Criticality: High

PossibleDamage: Non-compliance penalties and reputational damage

Category: Compliance

RiskType: Current

BusinessImpact: Legal penalties, reputational damage, regulatory fines

RiskDescription: Failure to document conservation efforts may result in non-compliance penalties and

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly update conservation documentation", "2": "Conduct internal audits on c

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 1919:

RiskId: 526

ComplianceId: 538

RiskTitle: Increased Waste Generation and Environmental Impact

Criticality: High

PossibleDamage: Increased waste disposal costs and regulatory fines

Category: Environmental
RiskType: Current
BusinessImpact: All business units within the Agriculture, Food, and Forest Products Group
RiskDescription: Failure to implement waste management plan could lead to higher waste generation,
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting of waste generation and recycling rates", "2": "In
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1920:
RiskId: 527
ComplianceId: 539
RiskTitle: Ineffective Waste Management Strategies
Criticality: Medium
PossibleDamage: Missed recycling targets and increased residual waste generation
Category: Environmental
RiskType: Current
BusinessImpact: All business units within the Agriculture, Food, and Forest Products Group
RiskDescription: Failure to review the waste management plan quarterly may result in ineffective waste
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing clear review processes and timelines", "2": "Regular communication
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1921:
RiskId: 528
ComplianceId: 540
RiskTitle: Inadequate Oversight of Climate-Related Risks
Criticality: High
PossibleDamage: Missed opportunities, increased risks, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Compromised decision-making processes, potential financial losses
RiskDescription: Failure to provide timely and accurate reports on climate-related risks may lead to uni
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting timelines and expectations", "2": "Provide training to CR
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 1922:
RiskId: 529
ComplianceId: 541
RiskTitle: Lack of Integration of Climate-Related Risks into Strategic Decision-Making
Criticality: Medium
PossibleDamage: Missed opportunities, increased risks, strategic misalignment
Category: Strategic
RiskType: Current
BusinessImpact: Potential negative impacts on long-term sustainability and competitiveness
RiskDescription: Failure to consider climate-related risks in strategic decision-making may lead to miss

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Include climate-related risk assessments in strategic planning sessions", "2": "Pro
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 1923:
RiskId: 530
ComplianceId: 542
RiskTitle: Ineffective Climate Risk Oversight
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of business operations, loss of investor confidence
RiskDescription: Failure to establish a climate risk management committee may result in inadequate ov
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular committee meetings to review climate risks", "2": "Develop comprehensiv
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 1924:
RiskId: 531

ComplianceId: 543
RiskTitle: Financial Impact of Unidentified Climate-Related Risks
Criticality: High
PossibleDamage: Financial losses due to unforeseen climate-related risks affecting the bank's operatio
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, reputational damage, and regulatory penalties
RiskDescription: Failure to identify and assess climate-related risks may result in financial losses due t
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct annual assessment as required", "2": "Implement risk management strat
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1925:
RiskId: 532
ComplianceId: 544
RiskTitle: Non-Compliance with Climate-Related Financial Disclosure Requirements
Criticality: High
PossibleDamage: Regulatory fines, loss of investor trust, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Financial penalties, decreased investor confidence
RiskDescription: Failure to include accurate and timely climate-related financial disclosures in annual r
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of compliance with TCFD guidelines", "2": "Internal audit of fin
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1926:
RiskId: 533
ComplianceId: 545
RiskTitle: Failure to Conduct Annual Assessment of Climate-Related Risks
Criticality: High
PossibleDamage: Inadequate risk management and financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may experience financial losses and reputational damage
RiskDescription: Failure to conduct annual assessments of climate-related risks may result in the orga
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust risk assessment process", "2": "Regularly review and update
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1927:
RiskId: 534
ComplianceId: 546
RiskTitle: Financial Impact of Climate-Related Events
Criticality: High
PossibleDamage: Financial losses, regulatory fines, and reputational damage

Category: Environmental
RiskType: Inherent
BusinessImpact: Significant financial impact on the organization
RiskDescription: Climate-related events such as extreme weather conditions or regulatory changes cou
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Diversification of investments to hedge against climate risks", "2": "Insurance cove
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1928:
RiskId: 535
ComplianceId: 547
RiskTitle: Inaccurate Climate-Related Risk Assessment
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory non-compliance
Category: Operational
RiskType: Inherent
BusinessImpact: All business units may be impacted by inaccurate risk assessment and missed oppor
RiskDescription: Failure to develop and disclose accurate climate-related metrics may lead to inaccura
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for the Sustainability and Reporting Te
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1929:
RiskId: 536
ComplianceId: 548
RiskTitle: Non-disclosure of Climate Metrics
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor confidence
Category: Compliance
RiskType: Current
BusinessImpact: Financial penalties, loss of business opportunities, damage to reputation
RiskDescription: Failure to disclose climate metrics can result in regulatory non-compliance and reputa
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting processes", "2": "Regular training on reporting requireme
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1930:
RiskId: 537
ComplianceId: 549
RiskTitle: Inaccurate GHG Emissions Reporting
Criticality: High
PossibleDamage: Potential regulatory fines and reputational damage
Category: Environmental
RiskType: Current
BusinessImpact: Non-compliance may lead to legal consequences and damage to the bank's reputatio
RiskDescription: Failure to accurately report GHG emissions could result in regulatory penalties and lo

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GHG Protocol methodology", "2": "Internal audits to verify calc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1931:
RiskId: 538
ComplianceId: 550
RiskTitle: Incorrect GHG Emissions Data Verification
Criticality: Medium
PossibleDamage: Potential regulatory fines and inaccurate reporting
Category: Environmental
RiskType: Current
BusinessImpact: Non-compliance may result in inaccurate reporting and regulatory penalties
RiskDescription: Failure to verify GHG emissions data accurately may lead to incorrect reporting and re
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Engage reputable external auditors", "2": "Implement regular audits of verification
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1932:
RiskId: 539

ComplianceId: 551
RiskTitle: Non-Compliance with Climate-Related Targets Description
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, stakeholder distrust
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of investor confidence, increased regulatory scrutiny
RiskDescription: Failure to comply with climate-related target setting and reporting requirements may r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of target setting and reporting processes", "2": "Engagement v
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1933:
RiskId: 540
ComplianceId: 552
RiskTitle: Inaccurate Reporting of GHG Emissions
Criticality: High
PossibleDamage: May result in reputational damage and regulatory fines
Category: Environmental
RiskType: Current
BusinessImpact: Potential impact on bank's reputation and credibility in sustainability efforts
RiskDescription: Failure to accurately report GHG emissions can lead to public scrutiny, loss of investo
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for staff on PCAF Standard implementation", "2": "Integ
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1934:
RiskId: 541
ComplianceId: 553
RiskTitle: Lack of Board Awareness on Climate-Related Risks
Criticality: High
PossibleDamage: Uninformed decision-making leading to increased exposure to climate-related risks
Category: Operational
RiskType: Current
BusinessImpact: Potential negative impact on business strategy and financial performance
RiskDescription: Failure to provide timely updates to the board may result in uninformed decision-maki
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely and accurate reporting by the Chief Risk Officer", "2": "Implement r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1935:
RiskId: 542
ComplianceId: 554
RiskTitle: Inadequate Oversight of Climate Risk Management Committee
Criticality: High
PossibleDamage: Financial losses, reputational damage, and regulatory non-compliance

Category: Operational
RiskType: Inherent
BusinessImpact: All business units would be affected by the consequences of inadequate oversight
RiskDescription: Failure to establish the climate risk management committee may result in insufficient a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication of committee roles and responsibilities", "2": "Provid
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1936:
RiskId: 543
ComplianceId: 555
RiskTitle: Missed Climate-Related Risks Assessment
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Environmental
RiskType: Inherent
BusinessImpact: Operational disruptions, decreased financial performance
RiskDescription: Failure to conduct the annual assessment of climate-related risks may result in the or
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Timely completion of assessments", "2": "Resource allocation for assessment", "3
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1937:
RiskId: 544
ComplianceId: 556
RiskTitle: Unanticipated Financial Impact of Climate Risks
Criticality: High
PossibleDamage: Financial losses due to unanticipated climate-related impacts
Category: Financial
RiskType: Residual
BusinessImpact: Potential budget overruns or revenue shortfalls
RiskDescription: Failure to incorporate climate risks into budgeting processes may result in financial los
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular climate risk assessments during budgeting", "2": "Scenario planning for e
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1938:
RiskId: 545
ComplianceId: 557
RiskTitle: Reputational Damage from Inadequate Climate Risk Management
Criticality: Medium
PossibleDamage: Reputational damage and financial losses due to inadequate climate risk manageme
Category: Reputational
RiskType: Residual
BusinessImpact: Loss of stakeholder trust and potential financial repercussions
RiskDescription: Failure to review financial plans for climate risks may lead to reputational damage and

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Annual climate risk training for board members", "2": "External climate risk audit o
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1939:
RiskId: 546
ComplianceId: 558
RiskTitle: Inadequate Climate Risk Assessment
Criticality: High
PossibleDamage: Financial losses and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Underwriting activities and financial performance
RiskDescription: Failure to accurately assess climate risks could result in underwriting losses and dam
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on climate risk analysis", "2": "Continuous monitoring of climate c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1940:
RiskId: 547

ComplianceId: 559
RiskTitle: Inadequate Integration of Climate Risks into Risk Management Framework
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to integrate climate risks into the risk management framework may result in ina
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on climate-related risks", "2": "Establish
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1941:
RiskId: 548
ComplianceId: 560
RiskTitle: Non-Disclosure of Climate-Related Metrics and Targets
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor trust
Category: Compliance
RiskType: Current
BusinessImpact: Financial reporting, investor relations, corporate governance
RiskDescription: Failure to disclose key metrics and targets related to climate-related risks and opportu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement robust data collection and reporting processes", "2": "Conduct regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1942:
RiskId: 549
ComplianceId: 561
RiskTitle: Non-Disclosure of Annual Expected Losses
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, financial losses
Category: Compliance
RiskType: Current
BusinessImpact: Financial instability, loss of stakeholder trust
RiskDescription: Failure to disclose accurate annual expected losses from weather-related catastrophe
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust risk assessment tools", "2": "Regularly review and update disclo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1943:
RiskId: 550
ComplianceId: 562
RiskTitle: Inaccurate Reporting of Greenhouse Gas Emissions
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of stakeholder trust

Category: Environmental
RiskType: Current
BusinessImpact: Negative impact on sustainability performance and stakeholder relationships
RiskDescription: Incorrect reporting of emissions data leading to misinformed decision-making and nor
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GHG Protocol methodology", "2": "Internal audits to verify data
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1944:
RiskId: 551
ComplianceId: 563
RiskTitle: Non-Disclosure of Climate-Related Targets
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor confidence
Category: Compliance
RiskType: Current
BusinessImpact: Negative impact on stakeholder trust and perception of the company's commitment to
RiskDescription: Failure to disclose climate-related targets and performance metrics can lead to regula
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting processes and timelines for target disclosure", "2": "Regu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1945:
RiskId: 552
ComplianceId: 564
RiskTitle: Ineffective Climate Risk Oversight
Criticality: High
PossibleDamage: Financial losses, reputational damage, missed opportunities
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage due to mismanagement of climate
RiskDescription: Failure to establish clear roles for oversight may result in inadequate monitoring and r
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for board members and management",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1946:
RiskId: 553
ComplianceId: 565
RiskTitle: Undetected Climate Risks
Criticality: High
PossibleDamage: Financial losses and reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Impacts investment performance and stakeholder trust
RiskDescription: Failure to detect climate risks may lead to incorrect investment decisions and negative

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular climate risk assessments", "2": "Utilize data analytics tools", "3": "Implem
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1947:
RiskId: 554
ComplianceId: 566
RiskTitle: Inadequate Climate Risk Assessment
Criticality: High
PossibleDamage: Financial losses, reputational damage, and regulatory penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Potential disruptions to operations, supply chain, and strategic decision-making
RiskDescription: Failure to assess climate-related risks may result in the organization being unprepare
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update climate risk assessment methodologies based on industry best
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1948:
RiskId: 555

ComplianceId: 567
RiskTitle: Financial Losses from Unanticipated Climate Risks
Criticality: High
PossibleDamage: Significant financial losses due to inadequate consideration of climate risks in financ
Category: Financial
RiskType: Inherent
BusinessImpact: Negative impact on budgeting, forecasting, and investment decisions
RiskDescription: Failure to integrate climate risks may result in unexpected financial losses, missed inv
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update climate risk assessments", "2": "Diversify investment portfolio to
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1949:
RiskId: 556
ComplianceId: 568
RiskTitle: Inadequate Scenario Analysis
Criticality: High
PossibleDamage: Financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to conduct biennial scenario analysis may result in inadequate preparedness f
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Ensure timely scheduling and completion of biennial scenario analysis", "2": "Eng
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1950:
RiskId: 557
ComplianceId: 569
RiskTitle: Inadequate Assessment of Climate Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory non-compliance
Category: Environmental
RiskType: Inherent
BusinessImpact: All business units may experience financial losses and reputational damage.
RiskDescription: Failure to accurately assess climate risks may result in inadequate mitigation strategie
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on climate risk assessment methodolo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1951:
RiskId: 558
ComplianceId: 570
RiskTitle: Inaccurate GHG Emissions Reporting
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of stakeholder trust

Category: Environmental
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation
RiskDescription: Failure to accurately report GHG emissions may lead to regulatory fines, reputational
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular internal audits to verify data accuracy", "2": "Provide training to s
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1952:
RiskId: 559
ComplianceId: 571
RiskTitle: Failure to Establish Climate-related Targets
Criticality: High
PossibleDamage: Missed sustainability goals, reputational damage
Category: Environmental
RiskType: Inherent
BusinessImpact: Loss of investor confidence, legal implications
RiskDescription: Failure to establish climate-related targets may result in the organization falling short
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting on progress towards targets", "2": "Engagement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1953:
RiskId: 560
ComplianceId: 572
RiskTitle: Failure to Report Progress on Climate-related Targets
Criticality: Medium
PossibleDamage: Lack of transparency, stakeholder distrust
Category: Reputational
RiskType: Residual
BusinessImpact: Regulatory non-compliance, loss of stakeholder trust
RiskDescription: Failure to report progress against climate-related targets may result in a lack of transp
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting mechanisms and timelines", "2": "Engage with external s
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1954:
RiskId: 561
ComplianceId: 573
RiskTitle: Inaccurate Reporting of GHG Emissions
Criticality: High
PossibleDamage: Potential regulatory fines, reputational damage, loss of stakeholder trust
Category: Environmental
RiskType: Current
BusinessImpact: Financial penalties, increased scrutiny from regulators and stakeholders
RiskDescription: Failure to accurately assess and report Scope 3 GHG emissions may result in mislea

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and updates on GHG Protocol methodology and industry standar
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1955:
RiskId: 562
ComplianceId: 574
RiskTitle: Inaccurate Reporting of GHG Emissions Metrics
Criticality: High
PossibleDamage: Reputational harm, regulatory fines, loss of stakeholder trust
Category: Compliance
RiskType: Residual
BusinessImpact: Potential loss of credibility and trust from stakeholders
RiskDescription: Failure to disclose accurate GHG emissions metrics can lead to misinformed decision
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on reporting methodologies", "2": "Internal audits to ensure comp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1956:
RiskId: 563

ComplianceId: 575
RiskTitle: Non-disclosure of Board Oversight Processes
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, increased climate-related risks
Category: Compliance
RiskType: Residual
BusinessImpact: All business units may be impacted by increased climate-related risks
RiskDescription: Failure to disclose board oversight processes may lead to lack of transparency and ac
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for board members on climate-related issues", "2": "External aud
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1957:
RiskId: 564
ComplianceId: 576
RiskTitle: Misalignment of Climate-Related Responsibilities
Criticality: High
PossibleDamage: Inadequate climate risk management and missed sustainable growth opportunities
Category: Operational
RiskType: Inherent
BusinessImpact: Compromised decision-making and reporting processes
RiskDescription: Failure to assign specific climate-related responsibilities may result in confusion, lack
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on climate-related responsibilities", "2"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1958:
RiskId: 565
ComplianceId: 577
RiskTitle: Misalignment with Climate-related Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage
Category: Environmental
RiskType: Current
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to identify and disclose climate-related risks may result in misalignment with m
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on climate-related risk assessment", "2": "Engagement with exter
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1959:
RiskId: 566
ComplianceId: 578
RiskTitle: Missed Climate-related Opportunities
Criticality: High
PossibleDamage: Loss of competitive advantage and financial performance due to missed opportunitie

Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to identify and capitalize on climate-related opportunities may lead to decrease
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish proactive monitoring of climate trends", "2": "Engage with industry exper
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1960:
RiskId: 567
ComplianceId: 579
RiskTitle: Misalignment of Investment Strategies with Climate Risks
Criticality: High
PossibleDamage: Underperformance or financial losses due to inadequate consideration of climate risk
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, reputational damage, regulatory fines
RiskDescription: Failure to integrate climate risks could result in misaligned investment decisions and u
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular climate risk training for investment teams", "2": "External climate risk asse
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1961:
RiskId: 568
ComplianceId: 580
RiskTitle: Increased Exposure to Climate-Related Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to assess climate-related risks may lead to increased exposure to environmen
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on climate-related risks", "2": "Engage
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1962:
RiskId: 569
ComplianceId: 581
RiskTitle: Inaccurate KPIs for Climate-Related Risks
Criticality: High
PossibleDamage: Loss of investment value and missed opportunities for growth
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to establish accurate KPIs may lead to incorrect assessment of climate-relate

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and adjustment of KPIs", "2": "Engagement with external experts f
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1963:
RiskId: 570
ComplianceId: 582
RiskTitle: Delayed Reporting of Climate-Related Metrics
Criticality: Medium
PossibleDamage: Lack of visibility into risks and missed opportunities for strategic planning
Category: Operational
RiskType: Inherent
BusinessImpact: Potential delays in decision-making and missed growth opportunities
RiskDescription: Failure to review and report metrics on time may lead to uninformed decision-making
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing clear reporting processes and timelines", "2": "Regular data quality c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1964:
RiskId: 571

ComplianceId: 583
RiskTitle: Inaccurate Reporting of Greenhouse Gas Emissions
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, and loss of investor trust
Category: Environmental
RiskType: Current
BusinessImpact: May result in non-compliance penalties, decreased investor confidence, and negative
RiskDescription: Incorrect reporting of emissions data may lead to misleading information being provid
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GHG Protocol methodology", "2": "Internal audits to ensure da
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1965:
RiskId: 572
ComplianceId: 584
RiskTitle: Inaccurate Portfolio Alignment Disclosure
Criticality: High
PossibleDamage: Reputational damage and loss of investor trust
Category: Operational
RiskType: Inherent
BusinessImpact: Negative impact on investor confidence and potential loss of assets under manageme
RiskDescription: Failure to accurately disclose portfolio alignment with climate goals may result in nega
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement regular training on alignment assessment methodologies", "2": "Condu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1966:
RiskId: 573
ComplianceId: 585
RiskTitle: Failure to Meet Climate-Related Targets
Criticality: High
PossibleDamage: Loss of investor confidence, reputational harm, financial penalties
Category: Operational
RiskType: Current
BusinessImpact: Potential decrease in assets under management, difficulty attracting new investors, in
RiskDescription: Failure to achieve climate-related targets could result in negative perceptions of the fi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting on progress towards targets", "2": "Engagement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1967:
RiskId: 574
ComplianceId: 586
RiskTitle: Inaccurate Reporting on Climate-Related Targets
Criticality: Medium
PossibleDamage: Loss of stakeholder trust, reputational damage, regulatory scrutiny

Category: Operational
RiskType: Current
BusinessImpact: Potential decrease in investor confidence, negative impact on ESG ratings, regulatory
RiskDescription: Inaccurate reporting on climate-related targets could undermine the credibility of the fi
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing clear reporting processes and timelines", "2": "Regularly reviewing ar
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 1968:
RiskId: 575
ComplianceId: 587
RiskTitle: Inaccurate climate risk assessment
Criticality: High
PossibleDamage: Potential financial losses due to misjudged climate risks
Category: Operational
RiskType: Inherent
BusinessImpact: Negative impact on investment performance and client trust
RiskDescription: Failure to accurately assess climate risks may lead to investment decisions based on
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on TCFD methodologies", "2": "Utilization of advanced s
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 1969:
RiskId: 576
ComplianceId: 588
RiskTitle: Inaccurate Climate Risk Disclosure
Criticality: High
PossibleDamage: Loss of stakeholder trust, regulatory fines
Category: Compliance
RiskType: Inherent
BusinessImpact: Negative impact on investment decisions, reputational damage
RiskDescription: Failure to accurately disclose climate risk assessments may lead to misinformed stak
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on TCFD guidelines", "2": "Internal audits of disclosure processes
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 1970:
RiskId: 577
ComplianceId: 589
RiskTitle: Inaccurate GHG Emissions Reporting
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, and loss of investor confidence
Category: Environmental
RiskType: Current
BusinessImpact: Direct impact on financial reporting and sustainability goals
RiskDescription: Failure to accurately report GHG emissions can lead to legal and financial repercussi

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on PCAF guidelines", "2": "Internal audits to verify calculations", "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1971:
RiskId: 578
ComplianceId: 590
RiskTitle: Inaccurate Carbon Footprint Disclosure
Criticality: High
PossibleDamage: Financial penalties, reputational harm
Category: Compliance
RiskType: Current
BusinessImpact: Loss of investor trust, regulatory scrutiny
RiskDescription: Failure to accurately disclose carbon footprint data can lead to regulatory fines and da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement data validation processes", "2": "Engage with sustainability experts for
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1972:
RiskId: 579

ComplianceId: 591
RiskTitle: Inaccurate Reporting of GHG Emissions
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of investor trust
Category: Environmental
RiskType: Current
BusinessImpact: Financial and reputational damage
RiskDescription: Incorrect reporting of GHG emissions could lead to financial penalties, regulatory scru
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GHG accounting protocols and tools", "2": "Internal audits to e
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1973:
RiskId: 580
ComplianceId: 592
RiskTitle: Inaccurate Reporting of Carbon Emissions
Criticality: High
PossibleDamage: Risk of reputational damage, regulatory fines, and loss of stakeholder trust
Category: Environmental
RiskType: Current
BusinessImpact: Potential financial losses, legal consequences, and damage to brand reputation
RiskDescription: Failure to accurately report carbon emissions can lead to misleading information bein
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement robust data collection processes to ensure accurate reporting", "2": "C
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1974:
RiskId: 581
ComplianceId: 593
RiskTitle: Inaccurate Reporting of Exposure to Carbon-Related Assets
Criticality: High
PossibleDamage: Loss of investor trust, reputational damage, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Negative impact on investment decisions and stakeholder relationships
RiskDescription: Failure to accurately assess and disclose exposure to carbon-related assets can lead
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data collection processes", "2": "Regularly review exposure met
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1975:
RiskId: 582
ComplianceId: 594
RiskTitle: Delayed Reporting on Climate-related Risks
Criticality: High
PossibleDamage: Uninformed decision-making and missed opportunities to mitigate risks

Category: Operational
RiskType: Current
BusinessImpact: Compromised board decision-making and strategic planning
RiskDescription: Failure to provide timely updates on climate-related risks may lead to uninformed dec
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting timelines and expectations", "2": "Implement regular revi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1976:
RiskId: 583
ComplianceId: 595
RiskTitle: Lack of Integration of Climate-related Risks in Strategic Planning
Criticality: Medium
PossibleDamage: Missed opportunities and increased vulnerabilities
Category: Strategic
RiskType: Current
BusinessImpact: Strategic objectives may not align with emerging climate-related risks
RiskDescription: Failure to incorporate climate-related risks into strategic planning may result in misse
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Integrate climate-related risk assessments into strategic planning processes", "2"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 1977:
RiskId: 584
ComplianceId: 596
RiskTitle: Inadequate Oversight of Climate Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to establish the committee may result in inadequate assessment and manage
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure clear communication and understanding of committee roles and responsib
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 1978:
RiskId: 585
ComplianceId: 597
RiskTitle: Financial Impact of Climate-Related Risks
Criticality: High
PossibleDamage: Financial losses, decreased shareholder value, increased insurance costs
Category: Financial
RiskType: Inherent
BusinessImpact: Potential financial losses and decreased profitability
RiskDescription: Failure to identify and mitigate climate-related risks could lead to financial losses and

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement risk mitigation strategies based on assessment findings", "2": "Regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1979:
RiskId: 586
ComplianceId: 598
RiskTitle: Failure to Integrate Climate Risks
Criticality: High
PossibleDamage: Financial losses due to unanticipated climate-related risks impacting investment dec
Category: Financial
RiskType: Inherent
BusinessImpact: Finance Department, Strategy Team
RiskDescription: Failure to consider climate risks in financial planning could result in misinformed inves
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on climate risk identification and mitigation strategies", "2": "Cont
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 1980:
RiskId: 587

ComplianceId: 599
RiskTitle: Failure to Conduct Biannual Scenario Analysis
Criticality: High
PossibleDamage: Strategic decisions may be uninformed and vulnerable to climate-related risks
Category: Strategic
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Not conducting biannual scenario analysis may lead to strategic decisions being base
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely completion of biannual scenario analysis", "2": "Engage relevant tea
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1981:
RiskId: 588
ComplianceId: 600
RiskTitle: Failure to Assess Climate-related Risks Annually
Criticality: High
PossibleDamage: Inadequate understanding of climate-related risks and their potential impact on the c
Category: Environmental
RiskType: Current
BusinessImpact: Financial losses, reputational damage, regulatory non-compliance
RiskDescription: Failure to conduct the annual assessment may result in the organization being unprep
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Ensure timely updates to the assessment based on emerging risks", "2": "Regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1982:
RiskId: 589
ComplianceId: 601
RiskTitle: Ineffective Management of Climate-related Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory penalties
Category: Operational
RiskType: Inherent
BusinessImpact: All business units would be affected by the consequences of ineffective risk managem
RiskDescription: Failure to effectively manage climate-related risks may result in significant financial lo
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on risk management processes", "2": "Continuous monitoring of r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1983:
RiskId: 590
ComplianceId: 602
RiskTitle: Failure to Integrate Climate-related Risks
Criticality: High
PossibleDamage: Increased exposure to environmental risks, financial losses, and reputational damag

Category: Environmental
RiskType: Current
BusinessImpact: All business units may suffer financial losses and reputational damage
RiskDescription: Failure to integrate climate-related risks into the overall risk management framework r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on climate-related risk integration", "2": "Annual review
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 1984:
RiskId: 591
ComplianceId: 603
RiskTitle: Inaccurate GHG Emissions Reporting
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, and loss of stakeholder trust
Category: Environmental
RiskType: Current
BusinessImpact: Potential legal actions, decreased investor confidence, and negative public perceptio
RiskDescription: Failure to accurately report GHG emissions data may lead to regulatory non-compliar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular internal audits to verify data accuracy", "2": "Implement training p
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 1985:
RiskId: 592
ComplianceId: 604
RiskTitle: Incorrect GHG Emissions Calculation Methodology
Criticality: Medium
PossibleDamage: Inaccurate emissions data, misrepresentation of environmental impact, and legal lial
Category: Environmental
RiskType: Current
BusinessImpact: Misinformed decision-making, potential legal actions, and regulatory non-compliance
RiskDescription: Use of incorrect or outdated GHG Protocol methodology may lead to inaccurate emis
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide training on GHG Protocol methodology to relevant teams", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1986:
RiskId: 593
ComplianceId: 605
RiskTitle: Non-compliance with Climate-related Target Setting
Criticality: High
PossibleDamage: Increased environmental impact, regulatory fines, reputational damage
Category: Environmental
RiskType: Current
BusinessImpact: Loss of stakeholder trust, increased carbon footprint, regulatory fines
RiskDescription: Failure to establish climate-related targets may lead to increased environmental impa

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for employees on target-setting proces
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1987:
RiskId: 594
ComplianceId: 606
RiskTitle: Inaccurate Climate-related Disclosures
Criticality: High
PossibleDamage: Reputational damage, financial losses, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Finance, Risk Management, Sustainability departments
RiskDescription: Failure to comply with TCFD recommendations may result in inaccurate or incomplete
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for committee members", "2": "Externa
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 1988:
RiskId: 595

ComplianceId: 607
RiskTitle: Undetected Climate-related Financial Risks
Criticality: High
PossibleDamage: Financial losses due to unidentified climate-related risks impacting operations
Category: Operational
RiskType: Inherent
BusinessImpact: All business units within the organization
RiskDescription: Failure to identify and address major climate-related risks could lead to financial losse
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement risk assessment framework", "2": "Regularly review assessment findin
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 1989:
RiskId: 596
ComplianceId: 608
RiskTitle: Non-disclosure of Climate-related KPIs
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor confidence
Category: Compliance
RiskType: Residual
BusinessImpact: Negative impact on stakeholder trust, financial performance, and market perception
RiskDescription: Failure to disclose climate-related KPIs in financial filings may result in regulatory non
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of regulatory updates related to climate disclosure requiremer
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 1990:
RiskId: 597
ComplianceId: 609
RiskTitle: Non-compliance with GHG Emissions Reporting
Criticality: High
PossibleDamage: Legal actions, fines, reputational damage
Category: Environmental
RiskType: Current
BusinessImpact: Potential regulatory fines, loss of investor confidence, reputational harm
RiskDescription: Failure to disclose GHG emissions could result in legal actions, fines, and reputationa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data collection and verification processes", "2": "Engage with th
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 1991:
RiskId: 598
ComplianceId: 610
RiskTitle: Lack of Sustainability Officer Oversight
Criticality: Medium
PossibleDamage: Inaccurate reporting, non-compliance

Category: Operational
RiskType: Current
BusinessImpact: Inaccurate reporting, potential non-compliance with emissions disclosure requirement
RiskDescription: Failure of the Sustainability Officer to oversee emissions reporting could result in inac
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide regular training and updates to the Sustainability Officer on emissions rep
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 1992:
RiskId: 599
ComplianceId: 611
RiskTitle: Non-alignment of Financial Activities with Climate Scenarios
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor confidence
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, decreased market share, increased regulatory scrutiny
RiskDescription: Failure to align financial activities with climate scenarios may result in increased expo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training and awareness programs for staff on climate scenario
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1993:
RiskId: 600
ComplianceId: 612
RiskTitle: Late Submission of Reports
Criticality: Medium
PossibleDamage: Missed opportunities, delayed decision-making, non-compliance penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Delayed decision-making, missed opportunities, financial penalties
RiskDescription: Late submission of reports may lead to missed opportunities, delayed decision-makin
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting timelines and escalation procedures", "2": "Automate rep
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1994:
RiskId: 601
ComplianceId: 613
RiskTitle: Failure to Establish Climate-Related Targets
Criticality: High
PossibleDamage: Inadequate risk management and missed opportunities for improvement
Category: Environmental
RiskType: Inherent
BusinessImpact: All business units involved in climate risk management
RiskDescription: Failure to establish climate-related targets may result in the organization being ill-prep

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of climate-related performance metrics", "2": "Engagement wit
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1995:
RiskId: 602
ComplianceId: 614
RiskTitle: Inadequate Performance Reporting Against Targets
Criticality: Medium
PossibleDamage: Stakeholder distrust and regulatory non-compliance
Category: Environmental
RiskType: Inherent
BusinessImpact: All business units involved in climate risk management
RiskDescription: Failure to report performance against climate-related targets may result in stakeholde
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated reporting systems for timely and accurate data collection", "2": "Regul
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 1996:
RiskId: 603

ComplianceId: 615
RiskTitle: Inaccurate Climate Disclosures
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, financial losses
Category: Compliance
RiskType: Inherent
BusinessImpact: May impact decision-making, investor confidence, and regulatory compliance
RiskDescription: Failure to accurately disclose climate-related financial information may lead to legal a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for committee members on TCFD recommendations", "2": "Exter
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 1997:
RiskId: 604
ComplianceId: 616
RiskTitle: Impact of Extreme Weather Events
Criticality: High
PossibleDamage: Disruption of operations and potential financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: Significant disruption to business operations
RiskDescription: Extreme weather events such as hurricanes or floods could lead to property damage,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Develop contingency plans for extreme weather events", "2": "Invest in resilient in
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 1998:
RiskId: 605
ComplianceId: 617
RiskTitle: Inaccurate Measurement of Environmental Impact
Criticality: High
PossibleDamage: Misleading stakeholders, missed sustainability goals, regulatory fines
Category: Environmental
RiskType: Current
BusinessImpact: Could lead to loss of credibility, decreased investor confidence, and regulatory scrutir
RiskDescription: Failure to accurately measure environmental impact can result in misinformed decisio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update KPIs to ensure relevance", "2": "Engage external au
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 1999:
RiskId: 606
ComplianceId: 618
RiskTitle: Outdated Climate Metrics and Targets
Criticality: Medium
PossibleDamage: Inaccurate reporting, missed sustainability goals, decreased investor confidence

Category: Operational
RiskType: Current
BusinessImpact: Could lead to misinformed decision-making, regulatory non-compliance, and reputatio
RiskDescription: Failure to review and update climate metrics and targets annually may result in inaccu
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear guidelines for updating metrics and targets", "2": "Engage external
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2000:
RiskId: 607
ComplianceId: 619
RiskTitle: Inaccurate Climate-related Disclosures
Criticality: High
PossibleDamage: Reputational damage, legal implications, loss of investor confidence
Category: Compliance
RiskType: Inherent
BusinessImpact: Financial performance, stakeholder trust
RiskDescription: Failure to accurately assess materiality for climate-related issues may result in mislea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear criteria for materiality assessment", "2": "Provide training to financ
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2001:
RiskId: 608
ComplianceId: 620
RiskTitle: Inaccurate Climate-related Disclosures
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor trust
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal implications, decreased investor confidence
RiskDescription: Failure to accurately disclose climate-related financial information can lead to legal ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear review processes", "2": "Engage external experts for validation", "3
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2002:
RiskId: 609
ComplianceId: 621
RiskTitle: Non-Compliance with GHG Emissions Reporting
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of investor confidence
Category: Environmental
RiskType: Current
BusinessImpact: Financial penalties, increased scrutiny, reputational harm
RiskDescription: Failure to comply with reporting requirements could result in legal action, fines, and da

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data collection and verification processes", "2": "Engage extern
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2003:
RiskId: 610
ComplianceId: 622
RiskTitle: Incomplete Disclosure of Scope 3 Emissions
Criticality: Medium
PossibleDamage: Stakeholder distrust, regulatory scrutiny, reputational damage
Category: Environmental
RiskType: Current
BusinessImpact: Loss of credibility, regulatory fines, reputational harm
RiskDescription: Failure to report material Scope 3 emissions could lead to incomplete disclosure, stak
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop clear criteria for assessing materiality of Scope 3 emissions", "2": "Engag
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2004:
RiskId: 611

ComplianceId: 623
RiskTitle: Unidentified Transition Risks
Criticality: High
PossibleDamage: Financial instability and loss of investment opportunities
Category: Financial
RiskType: Current
BusinessImpact: Financial losses impacting all business units
RiskDescription: Failure to identify transition risks could lead to missed opportunities for sustainable inv
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement risk management strategies based on assessment findings", "2": "Reg
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2005:
RiskId: 612
ComplianceId: 624
RiskTitle: Financial Impact Uncertainty
Criticality: High
PossibleDamage: Inaccurate financial decision-making, potential financial losses
Category: Financial
RiskType: Inherent
BusinessImpact: May lead to misallocation of resources, missed opportunities, and financial instability.
RiskDescription: Uncertainty in assessing the financial impacts of climate-related risks and opportunitie
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training on financial modeling techniques", "2": "External audit of financia
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2006:
RiskId: 613
ComplianceId: 625
RiskTitle: Non-compliance with Climate-Related Financial Reporting Regulations
Criticality: High
PossibleDamage: Financial penalties, reputational damage, loss of investor trust
Category: Operational
RiskType: Current
BusinessImpact: Delayed financial reporting, increased regulatory scrutiny, loss of investor confidence
RiskDescription: Failure to integrate climate-related financial impacts into annual reports may result in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on TCFD recommendations", "2": "External audits to verify comp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2007:
RiskId: 614
ComplianceId: 626
RiskTitle: Failure to Identify Regulatory Changes
Criticality: High
PossibleDamage: Non-compliance penalties and reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses and legal implications
RiskDescription: Failure to identify and adapt to regulatory changes may result in penalties and loss of
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular regulatory updates", "2": "Engage legal counsel for compliance checks", "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2008:
RiskId: 615
ComplianceId: 627
RiskTitle: Inaccurate Reporting of Climate-Related Impacts
Criticality: High
PossibleDamage: Misguided decision-making, regulatory fines, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, missed opportunities for improvement
RiskDescription: Failure to accurately monitor and report climate-related impacts may lead to misguide
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular data validation checks", "2": "Cross-departmental data verification proces
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2009:
RiskId: 616
ComplianceId: 628
RiskTitle: Inadequate Scenario Analysis
Criticality: High
PossibleDamage: Financial losses, missed opportunities, and strategic misalignment
Category: Operational
RiskType: Inherent
BusinessImpact: Direct impact on financial and sustainability functions
RiskDescription: Failure to conduct scenario analysis may result in inadequate understanding of climat
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a robust scenario analysis framework", "2": "Ensure timely review and
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2010:
RiskId: 617
ComplianceId: 629
RiskTitle: Inaccurate Risk Assessments due to Climate-Related Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Impact on decision-making, resource allocation, and strategic planning
RiskDescription: Failure to integrate climate-related risks may lead to inaccurate risk assessments, res

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on climate-related risks for risk management staff", "2": "Utilizatic
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2011:
RiskId: 618
ComplianceId: 630
RiskTitle: Inadequate Metrics and Targets
Criticality: High
PossibleDamage: Inefficient progress tracking and hindered transition towards a low-carbon economy
Category: Operational
RiskType: Current
BusinessImpact: Potential negative impact on sustainability and financial performance
RiskDescription: Failure to establish clear metrics and targets may lead to ineffective planning and exe
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and review of metrics and targets", "2": "Engagement with ind
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2012:
RiskId: 619

ComplianceId: 631
RiskTitle: Non-Disclosure of Progress
Criticality: Medium
PossibleDamage: Lack of stakeholder trust and transparency in sustainability efforts
Category: Reputational
RiskType: Current
BusinessImpact: Potential negative impact on reputation and stakeholder relationships
RiskDescription: Failure to disclose progress towards transition plans annually may lead to decreased
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting timelines and responsibilities", "2": "Engage with externa
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2013:
RiskId: 620
ComplianceId: 632
RiskTitle: Data Breach Risk Due to Lack of Access Control Policy
Criticality: High
PossibleDamage: Potential data loss, reputational damage, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial penalties, and damage to organizational repu
RiskDescription: Lack of a comprehensive access control policy may lead to unauthorized access, data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Employee training on policy implement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2014:
RiskId: 621
ComplianceId: 633
RiskTitle: Inconsistencies in Access Control Policy Management
Criticality: Medium
PossibleDamage: Delays, gaps, and inconsistencies in policy implementation
Category: Operational
RiskType: Residual
BusinessImpact: Challenges in policy adherence and potential gaps in access control implementation.
RiskDescription: Lack of a designated manager for access control policy may result in inconsistencies,
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear role definition and responsibilities", "2": "Regular performance evaluations c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2015:
RiskId: 622
ComplianceId: 634
RiskTitle: Unauthorized Access and Data Breach Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, and compliance violati

Category: Operational
RiskType: Current
BusinessImpact: All business units could suffer financial and reputational damage
RiskDescription: Unauthorized access to sensitive data could lead to data breaches, financial losses, a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of account types", "2": "Training for account managers
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2016:
RiskId: 623
ComplianceId: 635
RiskTitle: Unauthorized Account Creation Risk
Criticality: Medium
PossibleDamage: Unauthorized account creation, unauthorized access, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: All business units could suffer financial and reputational damage
RiskDescription: Unauthorized account creation could lead to unauthorized access, compliance violatio
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear approval processes for account creation", "2": "Regular audit of ac
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2017:
RiskId: 624
ComplianceId: 636
RiskTitle: Account Usage Monitoring Risk
Criticality: High
PossibleDamage: Unauthorized access, data breaches, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: All business units could suffer financial and reputational damage
RiskDescription: Failure to monitor account usage could lead to undetected unauthorized access, data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implementation of automated account monitoring tools", "2": "Regular review of a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2018:
RiskId: 625
ComplianceId: 637
RiskTitle: Unauthorized System Access
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, reputational damage
RiskDescription: Unauthorized users gaining access to sensitive systems and data, leading to potentia

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls", "2": "Regularly monitor account activity", "3": "Ir
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2019:
RiskId: 626
ComplianceId: 638
RiskTitle: Unusual Account Activity
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive data, reputational damage
RiskDescription: Failure to detect and respond to unusual account activities could lead to data breache
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement behavior analytics tools", "2": "Regularly train staff on detecting unusua
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2020:
RiskId: 627

ComplianceId: 639
RiskTitle: Data Breach due to Unauthorized Account Access
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal consequences
RiskDescription: Unauthorized access to critical systems and data resulting in potential data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security training for employees", "2": "Implementing data loss prevention
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2021:
RiskId: 628
ComplianceId: 640
RiskTitle: Unauthorized Access Due to Expired Accounts
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Failure to disable expired accounts may lead to unauthorized access to the system ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Regularly monitor and disable expired accounts", "2": "Implement automated acc

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 2022:

RiskId: 629

ComplianceId: 641

RiskTitle: Unauthorized Access Due to Inactive Accounts

Criticality: Medium

PossibleDamage: Data breaches, loss of sensitive information

Category: Operational

RiskType: Residual

BusinessImpact: All business units

RiskDescription: Failure to disable inactive accounts may lead to unauthorized access to the system a

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly monitor and disable inactive accounts", "2": "Implement automated acc

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 2023:

RiskId: 630

ComplianceId: 642

RiskTitle: Unauthorized Access Risk

Criticality: High

PossibleDamage: Data breaches and loss of sensitive information

Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust and financial penalties
RiskDescription: Failure to audit account creation actions could lead to unauthorized access to critical s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly review access logs", "3": "E
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2024:
RiskId: 631
ComplianceId: 643
RiskTitle: Unauthorized Changes Risk
Criticality: Medium
PossibleDamage: Unauthorized changes to account permissions
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations and potential data breaches
RiskDescription: Failure to audit account modification actions could lead to unauthorized changes in ac
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement segregation of duties", "2": "Regularly review access logs", "3": "Enforc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2025:
RiskId: 632
ComplianceId: 644
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, damage to reputation
RiskDescription: Unauthorized access to inactive user accounts can lead to data breaches and compro
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Regularly review and update access c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2026:
RiskId: 633
ComplianceId: 645
RiskTitle: Unauthorized Access to Sensitive Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial losses, reputational damage
RiskDescription: Unauthorized access to privileged user accounts can lead to data breaches, financial

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of role-based access permissions", "2": "Implement m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2027:
RiskId: 634
ComplianceId: 646
RiskTitle: Unauthorized Changes to Privileged Role Assignments
Criticality: Medium
PossibleDamage: Data breaches, compliance violations
Category: IT
RiskType: Residual
BusinessImpact: Potential unauthorized access to sensitive data, compliance violations
RiskDescription: Unauthorized changes to privileged role assignments can lead to data breaches and c
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated monitoring tools for privileged role assignments", "2": "Regu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2028:
RiskId: 635

ComplianceId: 647
RiskTitle: Unauthorized Access and Data Breach Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, legal implications, damage to reputation
RiskDescription: The risk of unauthorized access and data breaches due to shared and group account
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication mechanisms for shared accounts", "2": "Regularl
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2029:
RiskId: 636
ComplianceId: 648
RiskTitle: Data Breach Due to Undetected Atypical Usage
Criticality: High
PossibleDamage: Potential loss of sensitive data, damage to reputation, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines, legal consequences
RiskDescription: Failure to monitor atypical usage may result in undetected rogue behavior or ongoing
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools", "2": "Regularly review and update atypica
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2030:
RiskId: 637
ComplianceId: 649
RiskTitle: Delayed Response to Threats Due to Failure to Report Atypical Usage
Criticality: Medium
PossibleDamage: Continued malicious activities, potential data breaches, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial losses, legal consequences
RiskDescription: Failure to report atypical usage may result in delayed response to potential threats, al
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting procedures", "2": "Provide training to designated personn
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2031:
RiskId: 638
ComplianceId: 650
RiskTitle: Unauthorized Access Due to High-risk Individual Accounts
Criticality: High
PossibleDamage: Unauthorized access leading to data breaches, system disruptions, or financial losse

Category: Operational
RiskType: Current
BusinessImpact: All business units would be impacted by unauthorized access and potential harm cau
RiskDescription: Failure to disable high-risk individual accounts promptly may result in unauthorized ac
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of user activities", "2": "Automated alerts for suspicious behav
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2032:
RiskId: 639
ComplianceId: 651
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, compromised system
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial losses, reputational damage
RiskDescription: Unauthorized access to information and system resources can lead to data breaches,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews and audits", "2": "Implement multi-factor authentication",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2033:
RiskId: 640
ComplianceId: 652
RiskTitle: Data Breach Due to Lack of Information Flow Control
Criticality: High
PossibleDamage: Loss of sensitive information, regulatory fines, reputational damage.
Category: Operational
RiskType: Inherent
BusinessImpact: Potential loss of intellectual property, customer data, and financial information.
RiskDescription: Failure to enforce information flow control policies may lead to unauthorized access to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits and monitoring of information flow control mechanisms", "2": "Emp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2034:
RiskId: 641
ComplianceId: 653
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, loss of data integrity, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, damage to reputation
RiskDescription: Unauthorized access to sensitive information can lead to data breaches, loss of data i

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls and encryption mechanisms", "2": "Regularly m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2035:
RiskId: 642
ComplianceId: 654
RiskTitle: Data Breaches due to Physical Security Breaches
Criticality: Medium
PossibleDamage: Loss of data confidentiality, financial losses, damage to reputation
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of IT services, financial losses, damage to reputation
RiskDescription: Physical security breaches can lead to unauthorized access to sensitive information,
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement physical access controls and segregation of networks", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2036:
RiskId: 643

ComplianceId: 655
RiskTitle: Unauthorized Access Due to Lack of Duty Separation
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties, legal consequences
RiskDescription: Failure to identify and document duties requiring separation can lead to unauthorized
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls based on documented duties", "2": "Regularly re
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2037:
RiskId: 644
ComplianceId: 656
RiskTitle: Unauthorized Access Due to Undefined System Access Authorizations
Criticality: Medium
PossibleDamage: Unauthorized access to critical systems, data manipulation, system downtime
Category: IT
RiskType: Current
BusinessImpact: Disruption of critical systems, loss of data integrity, financial losses
RiskDescription: Lack of defined system access authorizations can lead to unauthorized access to criti
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement role-based access controls based on separation of duties", "2": "Regul
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2038:
RiskId: 645
ComplianceId: 657
RiskTitle: Data Breach due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage.
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, legal consequences.
RiskDescription: Unauthorized access to sensitive data can lead to data breaches, financial losses, an
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular access reviews", "2": "Enforce strong password policies", "3": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2039:
RiskId: 646
ComplianceId: 658
RiskTitle: Unauthorized Access to Security Functions
Criticality: High
PossibleDamage: Unauthorized access can lead to data breaches, system compromise, and loss of se

Category: IT
RiskType: Residual
BusinessImpact: All business units would be impacted by unauthorized access
RiskDescription: Unauthorized access to security functions and security-relevant information can result
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access control", "2": "Regularly review access permissions"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2040:
RiskId: 647
ComplianceId: 659
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, misuse of resources
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive information, financial loss, damage to reputation
RiskDescription: Unauthorized access to nonsecurity functions can lead to data breaches, misuse of re
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of access logs", "2": "Implementing multi-factor authentication
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2041:
RiskId: 648
ComplianceId: 660
RiskTitle: Unauthorized Access to Privileged Information
Criticality: High
PossibleDamage: Data breaches, system compromise
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, damage to reputation
RiskDescription: Unauthorized access to privileged information can lead to data breaches and compro
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access control for privileged accounts", "2": "Regularly revi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2042:
RiskId: 649
ComplianceId: 661
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Potential financial losses, reputational damage
RiskDescription: Unauthorized access to critical systems and data due to improperly assigned user pri

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews", "2": "Implementing role-based access control", "3": "Imp
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2043:
RiskId: 650
ComplianceId: 662
RiskTitle: Misuse of Privileged Functions
Criticality: High
PossibleDamage: Data breaches, system compromise, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: IT, Security
RiskDescription: Unauthorized use of privileged functions can lead to unauthorized access and compro
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review of privileged function logs", "2": "Implementation of anomaly detec
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2044:
RiskId: 651

ComplianceId: 663
RiskTitle: Unauthorized Access to Sensitive Data
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Non-privileged users gaining access to sensitive data can lead to data breaches, finar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls", "2": "Regularly monitor and audit user activities
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2045:
RiskId: 652
ComplianceId: 664
RiskTitle: Unauthorized System Changes
Criticality: Medium
PossibleDamage: System compromise, data integrity issues
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, compliance violations
RiskDescription: Non-privileged users making unauthorized changes to system settings can lead to sys
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement strict access control policies", "2": "Regularly audit and monitor system
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2046:
RiskId: 653
ComplianceId: 665
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Increased risk of unauthorized access and potential data breaches
Category: Operational
RiskType: Current
BusinessImpact: All business units would be impacted by unauthorized access
RiskDescription: Unauthorized access to sensitive information, data breaches, compromised user acco
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Implement multi-factor authentication",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2047:
RiskId: 654
ComplianceId: 666
RiskTitle: Denial of Service Risk
Criticality: High
PossibleDamage: Increased risk of unauthorized access and potential denial of service attacks

Category: Operational
RiskType: Current
BusinessImpact: All business units would be impacted by denial of service attacks
RiskDescription: Denial of service attacks, unauthorized access to sensitive information
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement account lockout policies", "2": "Implement monitoring for unusual logon
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2048:
RiskId: 655
ComplianceId: 667
RiskTitle: Unauthorized System Access
Criticality: High
PossibleDamage: Data breaches, legal penalties
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial losses
RiskDescription: Unauthorized users gaining access to the system due to lack of clear system use noti
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and review system use notification message to ensure compliar
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2049:
RiskId: 656
ComplianceId: 668
RiskTitle: Bypassed System Use Notification
Criticality: Medium
PossibleDamage: Data breaches, legal penalties
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial losses
RiskDescription: Users bypassing the system use notification message without acknowledging usage c
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated timeout for unacknowledged messages to prevent unautho
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2050:
RiskId: 657
ComplianceId: 669
RiskTitle: Misuse of Publicly Accessible Systems
Criticality: High
PossibleDamage: Misuse of system resources, legal liabilities
Category: Operational
RiskType: Residual
BusinessImpact: Potential misuse of system resources, legal disputes
RiskDescription: Users accessing publicly accessible systems without understanding authorized uses a

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update system use information for accuracy and compliance
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2051:
RiskId: 658
ComplianceId: 670
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, potential loss of intelle
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by unauthorized access to sensitive data
RiskDescription: Unauthorized access to organizational systems can lead to data breaches, loss of inte
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated device lock settings on all devices", "2": "Provide training to
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2052:
RiskId: 659

ComplianceId: 671
RiskTitle: User Compliance Risk
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information, data breaches, potential loss of intelle
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by unauthorized access to sensitive data
RiskDescription: Lack of user compliance with device locking procedures can lead to unauthorized acc
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enforce policy adherence through regular reminders and training", "2": "Implemen
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2053:
RiskId: 660
ComplianceId: 672
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Unauthorized access to controlled unclassified information due to lack of device lock a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Enforce strong password policies for device lock activation", "2": "Implement multi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2054:
RiskId: 661
ComplianceId: 673
RiskTitle: Display Privacy Risk
Criticality: Medium
PossibleDamage: Unauthorized viewing of sensitive information, data leaks
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Unauthorized viewing of controlled unclassified information due to improper use of pa
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly monitor display usage for compliance", "2": "Implement screen privacy f
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2055:
RiskId: 662
ComplianceId: 674
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, security incidents

Category: Operational
RiskType: Current
BusinessImpact: Potential loss of confidential data, financial losses, reputational damage
RiskDescription: Failure to automatically terminate user sessions may lead to unauthorized access and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement session timeout settings", "2": "Regularly review and update trigger ev
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2056:
RiskId: 663
ComplianceId: 675
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Risk of unauthorized individuals gaining access to sensitive information or systems du
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls for identified user actions", "2": "Regularly review
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2057:
RiskId: 664
ComplianceId: 676
RiskTitle: Accountability Gap Risk
Criticality: Medium
PossibleDamage: Lack of accountability, audit trail gaps, security vulnerabilities
Category: IT
RiskType: Residual
BusinessImpact: Specific business units
RiskDescription: Risk of lack of accountability and audit trail gaps due to user actions performed withou
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Maintain detailed records of rationale for each identified user action", "2": "Implem
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2058:
RiskId: 665
ComplianceId: 677
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, compromised system
Category: IT
RiskType: Residual
BusinessImpact: IT, Compliance
RiskDescription: Unauthorized access to sensitive data and compromised system integrity due to insec

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits and reviews of remote access configurations", "2": "Implement mu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2059:
RiskId: 666
ComplianceId: 678
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access, data breaches, compromised system security
Category: IT
RiskType: Residual
BusinessImpact: IT, Compliance
RiskDescription: Unauthorized access and compromised system security due to lack of proper authoriz
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access control mechanisms to enforce authorization", "2": "Regularly r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2060:
RiskId: 667

ComplianceId: 679
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, data breaches, compliance violations.
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial penalties, damage to reputation.
RiskDescription: Risk of unauthorized access to sensitive data through remote access methods leadin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for remote access", "2": "Regularly review a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2061:
RiskId: 668
ComplianceId: 680
RiskTitle: Audit Logging Non-Compliance Risk
Criticality: Medium
PossibleDamage: Non-compliance with audit logging requirements, inability to detect unauthorized acc
Category: Operational
RiskType: Residual
BusinessImpact: Risk of undetected unauthorized access and attacks due to lack of audit logging com
RiskDescription: Risk of non-compliance with audit logging requirements leading to the inability to dete
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regularly review audit logs for anomalies", "2": "Implement automated alerts for s
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2062:
RiskId: 669
ComplianceId: 681
RiskTitle: Data Breach Risk due to Lack of Encryption
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, financial losses, reputational damage
Category: IT
RiskType: Current
BusinessImpact: Financial losses, loss of customer trust, regulatory fines
RiskDescription: Failure to implement TLS encryption could lead to unauthorized access to sensitive d
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update TLS versions and configurations", "2": "Implement multi-factor a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2063:
RiskId: 670
ComplianceId: 682
RiskTitle: Risk of Encryption Key Loss
Criticality: Medium
PossibleDamage: Loss of encryption keys, unauthorized access to sensitive data

Category: IT
RiskType: Current
BusinessImpact: Loss of data confidentiality, potential data breaches
RiskDescription: Failure to securely manage encryption keys could result in their loss, leading to unaut
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement key rotation policies", "2": "Use hardware security modules for key sto
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2064:
RiskId: 671
ComplianceId: 683
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, network breaches, and potential data exfiltra
Category: Operational
RiskType: Residual
BusinessImpact: Potential data loss, reputational damage, financial losses.
RiskDescription: Unauthorized access to critical systems and data due to lack of proper routing through
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication mechanisms for remote access", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2065:
RiskId: 672
ComplianceId: 684
RiskTitle: Unauthorized Execution of Privileged Commands via Remote Access
Criticality: High
PossibleDamage: Data breaches, system compromise
Category: IT
RiskType: Current
BusinessImpact: IT systems and data integrity compromised
RiskDescription: Unauthorized execution of privileged commands via remote access could lead to una
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for remote access", "2": "Monitor and log all
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2066:
RiskId: 673
ComplianceId: 685
RiskTitle: Lack of Documentation for Remote Access Rationale
Criticality: Medium
PossibleDamage: Confusion, misuse of remote access capabilities
Category: IT
RiskType: Current
BusinessImpact: Confusion in remote access management, potential misuse of capabilities
RiskDescription: Lack of documentation for remote access rationale could lead to confusion or misuse

RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update the security plan with remote access rationale", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2067:
RiskId: 674
ComplianceId: 686
RiskTitle: Unauthorized Access to Wireless Network
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, network compromise
Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, damage to reputation
RiskDescription: Unauthorized individuals gaining access to the wireless network can lead to data brea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication mechanisms for wireless access", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2068:
RiskId: 675

ComplianceId: 687
RiskTitle: Unauthorized Access to Wireless Network Resources
Criticality: Medium
PossibleDamage: Data breaches, loss of sensitive information, unauthorized network access
Category: IT
RiskType: Current
BusinessImpact: Loss of confidential data, disruption of operations, financial losses
RiskDescription: Unauthorized access to wireless network resources can lead to data breaches, loss o
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement role-based access control for wireless connections", "2": "Regularly mo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2069:
RiskId: 676
ComplianceId: 688
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, system compromise
Category: IT
RiskType: Inherent
BusinessImpact: Loss of sensitive data, disruption of operations
RiskDescription: Unauthorized users gaining access to the system through unsecured wireless connec
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for wireless access", "2": "Regularly update
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2070:
RiskId: 677
ComplianceId: 689
RiskTitle: Data Interception Risk
Criticality: Medium
PossibleDamage: Data leakage, unauthorized access
Category: IT
RiskType: Inherent
BusinessImpact: Loss of sensitive data, compromised data integrity
RiskDescription: Data transmitted wirelessly without encryption can be intercepted by adversaries, lead
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement WPA3 encryption for wireless networks", "2": "Regularly audit encrypti
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2071:
RiskId: 678
ComplianceId: 690
RiskTitle: Unauthorized Access through Wireless Vulnerabilities
Criticality: High
PossibleDamage: Potential unauthorized access to sensitive information through wireless vulnerabilitie

Category: IT
RiskType: Residual
BusinessImpact: Data breaches, loss of sensitive information, reputational damage
RiskDescription: Adversaries exploiting wireless vulnerabilities could gain unauthorized access to sens
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly scan for unauthorized wireless access points", "2": "Implement network
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2072:
RiskId: 679
ComplianceId: 691
RiskTitle: Unauthorized Access to Sensitive Information on Mobile Devices
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, malware infections
Category: IT
RiskType: Residual
BusinessImpact: All business units would be impacted by potential data breaches and unauthorized ac
RiskDescription: Unauthorized access to sensitive information on organization-controlled mobile device
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies for mobile devices", "2": "Encrypt data stored
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2073:
RiskId: 680
ComplianceId: 692
RiskTitle: Unauthorized Access to Organizational Systems via Mobile Devices
Criticality: Medium
PossibleDamage: Unauthorized access to organizational systems, data breaches, malware infections
Category: IT
RiskType: Residual
BusinessImpact: All business units would be impacted by potential data breaches and unauthorized ac
RiskDescription: Unauthorized access to organizational systems via unauthorized mobile devices can
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement device identification and authentication mechanisms", "2": "Implement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2074:
RiskId: 681
ComplianceId: 693
RiskTitle: Data Breach Due to Lack of Encryption on Mobile Devices
Criticality: High
PossibleDamage: Loss of sensitive data, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Disruption of business operations, financial losses, damage to reputation
RiskDescription: Unauthorized access to sensitive information stored on mobile devices can lead to da

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption software and security patches", "2": "Enforce strong
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2075:
RiskId: 682
ComplianceId: 694
RiskTitle: Data Breach Due to Unauthorized Access to Encrypted Data Structures
Criticality: Medium
PossibleDamage: Loss of specific data structures, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of specific data structures, potential legal liabilities, damage to reputation
RiskDescription: Unauthorized access to specific data structures on mobile devices can lead to data br
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement data classification policies to identify sensitive data", "2": "Regularly au
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2076:
RiskId: 683

ComplianceId: 695
RiskTitle: Unauthorized Access to Organization-Controlled Information
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, regulatory fines, reputational damage
RiskDescription: Unauthorized individuals gaining access to organization-controlled information throug
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls and monitoring for external system access", "2": "Regu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2077:
RiskId: 684
ComplianceId: 696
RiskTitle: Use of Prohibited External Systems
Criticality: Medium
PossibleDamage: Security vulnerabilities, data breaches
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive information, regulatory non-compliance, reputational damage
RiskDescription: Unauthorized use of prohibited external systems that do not meet organization-define
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regularly update and communicate list of prohibited external systems", "2": "Impl
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2078:
RiskId: 685
ComplianceId: 697
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, compromise of organizational systems
Category: IT
RiskType: Residual
BusinessImpact: Potential data breaches, loss of sensitive information
RiskDescription: Risk of unauthorized individuals gaining access to organization-controlled information
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for external system access", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2079:
RiskId: 686
ComplianceId: 698
RiskTitle: System Connection Agreement Risk
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information, compromise of organizational systems

Category: IT
RiskType: Residual
BusinessImpact: Potential data breaches, loss of sensitive information
RiskDescription: Risk of authorized individuals accessing organization-controlled information without fo
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear guidelines for system connection agreements", "2": "Regularly rev
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2080:
RiskId: 687
ComplianceId: 699
RiskTitle: Data Breach through Portable Storage Devices
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, damage to reputation
RiskDescription: Unauthorized access to sensitive data stored on portable storage devices leading to d
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls on portable storage devices", "2": "Regularly m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2081:
RiskId: 688
ComplianceId: 700
RiskTitle: Unauthorized Sharing of Sensitive Information
Criticality: High
PossibleDamage: Data breaches, legal consequences, reputational damage.
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties, legal liabilities.
RiskDescription: Unauthorized sharing of sensitive information can lead to data breaches, legal conse
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls", "2": "Regular monitoring of access logs", "3": "E
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2082:
RiskId: 689
ComplianceId: 701
RiskTitle: Misinterpretation of Information Sharing Policies
Criticality: Medium
PossibleDamage: Accidental sharing of sensitive data, compliance violations.
Category: Operational
RiskType: Current
BusinessImpact: Compliance penalties, loss of sensitive data, reputational damage.
RiskDescription: Misinterpretation of information sharing policies can lead to accidental sharing of sens

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on information sharing policies", "2": "Implementing user-friendly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2083:
RiskId: 690
ComplianceId: 702
RiskTitle: Unauthorized Disclosure of Nonpublic Information
Criticality: High
PossibleDamage: Legal actions, fines, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Legal consequences, reputational damage, loss of customer trust
RiskDescription: Unauthorized individuals post nonpublic information on publicly accessible systems, v
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the list of authorized individuals", "2": "Provide ongo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2084:
RiskId: 691

ComplianceId: 703
RiskTitle: Unintentional Disclosure of Nonpublic Information
Criticality: Medium
PossibleDamage: Data breaches, legal actions, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Legal consequences, reputational damage, loss of customer trust
RiskDescription: Authorized individuals unknowingly post nonpublic information on publicly accessible
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide regular training sessions on identifying nonpublic information", "2": "Imple
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2085:
RiskId: 692
ComplianceId: 704
RiskTitle: Inadequate awareness and training policy
Criticality: High
PossibleDamage: Increased risk of security incidents or breaches
Category: Operational
RiskType: Current
BusinessImpact: All business units may face disruptions and reputational damage
RiskDescription: Failure to have a clear and comprehensive awareness and training policy may result i
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for all personnel on the awareness and training policy",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2086:
RiskId: 693
ComplianceId: 705
RiskTitle: Lack of designated official for policy management
Criticality: Medium
PossibleDamage: Inconsistent policy development and dissemination
Category: Operational
RiskType: Current
BusinessImpact: All business units may experience confusion and inefficiencies in awareness and trai
RiskDescription: Failure to designate an official for managing the awareness and training policy may re
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clearly define roles and responsibilities of the designated official", "2": "Provide ne
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2087:
RiskId: 694
ComplianceId: 706
RiskTitle: Outdated awareness and training policy and procedures
Criticality: High
PossibleDamage: Increased risk of security incidents or breaches

Category: Operational
RiskType: Current
BusinessImpact: All business units may face disruptions and security vulnerabilities
RiskDescription: Failure to review and update the awareness and training policy and procedures may r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a regular review schedule for policy and procedures", "2": "Include post-
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2088:
RiskId: 695
ComplianceId: 707
RiskTitle: Inadequate security and privacy literacy training
Criticality: High
PossibleDamage: Security incidents, breaches, non-compliance with laws and regulations
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential security incidents or breaches
RiskDescription: Failure to provide adequate literacy training may result in security incidents, breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update literacy training content based on assessment findings and char
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2089:
RiskId: 696
ComplianceId: 708
RiskTitle: Lack of security and privacy awareness
Criticality: Medium
PossibleDamage: Security incidents, breaches, non-compliance with security and privacy policies
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential security incidents or breaches
RiskDescription: Lack of awareness may lead to security incidents, breaches, or non-compliance with s
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 43.2
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update awareness techniques based on organizational events and char
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2090:
RiskId: 697
ComplianceId: 709
RiskTitle: Undetected Insider Threats
Criticality: High
PossibleDamage: Financial loss, data breaches, harm to employees
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial loss, reputational damage, and legal consequences
RiskDescription: Failure to detect insider threats may result in unauthorized access to sensitive informa

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust access controls and monitoring systems", "2": "Encourage a cu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2091:
RiskId: 698
ComplianceId: 710
RiskTitle: Employee Vulnerability to Social Engineering Attacks
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential loss of sensitive information, financial resources, and damage to reputation
RiskDescription: Employees unknowingly falling victim to social engineering attacks resulting in unauth
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular employee training on social engineering awareness", "2": "Implement mu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2092:
RiskId: 699

ComplianceId: 711
RiskTitle: Inadequate Role-based Training
Criticality: High
PossibleDamage: Increased security incidents, breaches, and non-compliance with regulations
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential security incidents and breaches.
RiskDescription: Failure to provide adequate role-based training may result in personnel not being equ
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update training content based on lessons learned from incid
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2093:
RiskId: 700
ComplianceId: 712
RiskTitle: Inadequate Documentation of Training Activities
Criticality: High
PossibleDamage: Increased risk of security and privacy incidents due to lack of proper training docume
Category: Operational
RiskType: Residual
BusinessImpact: Potential security breaches, data leaks, and non-compliance penalties.
RiskDescription: Failure to document training activities may result in employees not receiving necessar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement a centralized training documentation system", "2": "Regularly review a

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 2094:

RiskId: 701

ComplianceId: 713

RiskTitle: Non-Retention of Individual Training Records

Criticality: Medium

PossibleDamage: Inability to verify training completion and potential non-compliance with regulatory re

Category: Operational

RiskType: Residual

BusinessImpact: Risk of non-compliance penalties, security incidents due to untrained personnel.

RiskDescription: Lack of retained training records may lead to inability to verify employee training, resu

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Establish a clear retention policy for training records", "2": "Implement a secure st

CreatedAt: 2025-10-09 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 2095:

RiskId: 702

ComplianceId: 714

RiskTitle: Inadequate audit and accountability controls

Criticality: High

PossibleDamage: Increased risk of security incidents and breaches

Category: Operational
RiskType: Residual
BusinessImpact: Potential compromise of sensitive data, financial loss, reputational damage
RiskDescription: Failure to develop and disseminate audit and accountability policy may result in inade
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on audit and accountability policies", "2
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2096:
RiskId: 703
ComplianceId: 715
RiskTitle: Inconsistencies in policy management
Criticality: Medium
PossibleDamage: Lack of oversight and accountability
Category: Operational
RiskType: Residual
BusinessImpact: Potential confusion, delays, and errors in policy implementation
RiskDescription: Failure to designate an official for policy management may result in inconsistencies, le
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clearly define roles and responsibilities of the designated official", "2": "Provide ac
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2097:
RiskId: 704
ComplianceId: 716
RiskTitle: Incomplete Event Logging Identification
Criticality: High
PossibleDamage: Incomplete audit trails hindering incident investigations
Category: Operational
RiskType: Current
BusinessImpact: Inability to effectively investigate security incidents
RiskDescription: Failure to identify all relevant event types for logging may result in incomplete audit tra
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review of event types to ensure completeness", "2": "Engage with relevan
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2098:
RiskId: 705
ComplianceId: 717
RiskTitle: Lack of Coordination in Event Logging
Criticality: Medium
PossibleDamage: Inconsistencies in audit-related information hindering incident response efforts
Category: Operational
RiskType: Current
BusinessImpact: Inconsistencies in audit-related information may lead to delays in incident response a
RiskDescription: Failure to coordinate event logging with other organizational entities may result in inco

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels with other entities", "2": "Regularly review
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2099:
RiskId: 706
ComplianceId: 718
RiskTitle: Outdated Event Logging Practices
Criticality: High
PossibleDamage: Ineffective incident investigations due to outdated logging practices
Category: Operational
RiskType: Current
BusinessImpact: Outdated logging practices may lead to delays in identifying and resolving incidents.
RiskDescription: Failure to review and update event types selected for logging may result in outdated l
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a regular review schedule for event types", "2": "Engage with stakeholde
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2100:
RiskId: 707

ComplianceId: 719
RiskTitle: Inaccurate Event Description Risk
Criticality: High
PossibleDamage: Misinterpretation of audit records and potential compliance violations
Category: Compliance
RiskType: Residual
BusinessImpact: May lead to regulatory fines and reputational damage
RiskDescription: Failure to accurately describe events in audit records may result in misinterpretation b
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on event description standards", "2": "Implement automated ever
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2101:
RiskId: 708
ComplianceId: 720
RiskTitle: Incorrect Time Stamp Risk
Criticality: Medium
PossibleDamage: Audit discrepancies and potential compliance violations
Category: Compliance
RiskType: Residual
BusinessImpact: May lead to regulatory scrutiny and operational disruptions
RiskDescription: Inaccurate time stamps in audit records may result in incorrect event sequencing and
RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement automated time stamp synchronization tools", "2": "Regularly verify tim
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2102:
RiskId: 709
ComplianceId: 721
RiskTitle: Security Breach due to Missing Access Control Information
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Significant financial and reputational losses
RiskDescription: Failure to include access control rules in audit records may lead to unauthorized acce
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update access control rules in audit records", "2": "Implement multi-fact
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2103:
RiskId: 710
ComplianceId: 722
RiskTitle: Privacy Violations due to Inclusion of Unnecessary Information in Audit Records
Criticality: Medium
PossibleDamage: Legal repercussions, loss of customer trust, financial penalties

Category: Compliance
RiskType: Residual
BusinessImpact: Potential legal fines and loss of customer trust
RiskDescription: Inclusion of unnecessary information in audit records may violate privacy regulations a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update audit record content based on audit requirements", "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2104:
RiskId: 711
ComplianceId: 723
RiskTitle: Audit Log Storage Capacity Exceeded
Criticality: High
PossibleDamage: Loss of critical audit data, inability to track security incidents or compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Loss of critical audit data could lead to undetected security incidents and compliance
RiskDescription: If audit log storage capacity is exceeded, critical audit data may be lost, impacting the
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of audit log storage capacity", "2": "Implement automated aler
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2105:
RiskId: 712
ComplianceId: 724
RiskTitle: Delayed Response to Audit Logging Process Failures
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data manipulation, or system downtim
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches or system disruptions affecting all business units
RiskDescription: Failure to promptly alert personnel in case of audit logging process failures may lead t
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring systems for audit logs", "2": "Regularly test alert
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2106:
RiskId: 713
ComplianceId: 725
RiskTitle: Inadequate Response to Audit Logging Process Failures
Criticality: Medium
PossibleDamage: Prolonged system downtime, data loss, or security incidents
Category: Operational
RiskType: Current
BusinessImpact: All business units may be impacted by prolonged system downtime, data loss, or sec
RiskDescription: Failure to define and implement appropriate responses to audit logging process failure

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update response procedures based on evolving threats and
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2107:
RiskId: 714
ComplianceId: 726
RiskTitle: Undetected Security Breaches
Criticality: High
PossibleDamage: Undetected breaches may lead to data loss, financial losses, reputational damage, a
Category: Operational
RiskType: Current
BusinessImpact: IT, Security, Compliance
RiskDescription: Failure to detect security breaches in a timely manner can result in significant financia
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools for real-time analysis", "2": "Provide regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2108:
RiskId: 715

ComplianceId: 727
RiskTitle: Delayed Incident Response
Criticality: Medium
PossibleDamage: Delays in incident response can lead to prolonged security breaches, increased data
Category: Operational
RiskType: Current
BusinessImpact: IT, Security, Incident Response
RiskDescription: Failure to report audit findings in a timely manner can result in prolonged security inci
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting procedures and escalation paths", "2": "Regularly review
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2109:
RiskId: 716
ComplianceId: 728
RiskTitle: Incomplete Analysis of Audit Records
Criticality: High
PossibleDamage: Undetected security incidents or compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, damage to reputation, and legal consequences.
RiskDescription: Failure to integrate automated mechanisms for audit record review may result in incor
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular testing and validation of automated mechanisms", "2": "Implementing aut
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2110:
RiskId: 717
ComplianceId: 729
RiskTitle: Missed Security Incident Detection
Criticality: High
PossibleDamage: Undetected security incidents or breaches
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of sensitive data, damage to reputation, financial losses.
RiskDescription: Failure to correlate audit records may result in missed security incidents, breaches, or
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated correlation tools", "2": "Regularly review and update correla
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2111:
RiskId: 718
ComplianceId: 730
RiskTitle: Inaccurate Audit Data Analysis
Criticality: High
PossibleDamage: Missed anomalies or incidents, compromised incident investigations

Category: Operational
RiskType: Current
BusinessImpact: May lead to regulatory non-compliance, security breaches, or financial losses
RiskDescription: Failure to accurately analyze audit data due to inadequate record reduction and repor
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update audit record reduction algorithms", "2": "Conduct per
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2112:
RiskId: 719
ComplianceId: 731
RiskTitle: Missed Critical Event Detection
Criticality: High
PossibleDamage: Failure to detect critical events in audit records.
Category: Operational
RiskType: Current
BusinessImpact: Potential security breaches or compliance violations.
RiskDescription: Lack of clear reduction criteria may lead to overlooking important events in audit reco
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of audit record reduction criteria", "2": "Automated ale
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2113:
RiskId: 720
ComplianceId: 732
RiskTitle: Inefficient Incident Response
Criticality: Medium
PossibleDamage: Delays in identifying and responding to security incidents.
Category: IT
RiskType: Current
BusinessImpact: Potential data breaches or prolonged system downtime.
RiskDescription: Manual audit record search processes may hinder timely incident response efforts.
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular testing of automated search capabilities", "2": "Continuous monitoring of
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2114:
RiskId: 721
ComplianceId: 733
RiskTitle: Inaccurate Time Stamps
Criticality: High
PossibleDamage: Compromised audit trail analysis and security capabilities
Category: Operational
RiskType: Current
BusinessImpact: Potential unauthorized access or data breaches
RiskDescription: Failure to use internal system clocks for time stamps can result in inaccurate or unsyn

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated time synchronization mechanisms", "2": "Regularly monitor
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2115:
RiskId: 722
ComplianceId: 734
RiskTitle: Inconsistent Time Stamp Formats
Criticality: Medium
PossibleDamage: Confusion in audit trail analysis and hindered security capabilities
Category: Operational
RiskType: Current
BusinessImpact: Potential hindrance in security measures and audit trail analysis
RiskDescription: Failure to record time stamps with Coordinated Universal Time or consistent local tim
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Standardize time stamp formats across systems", "2": "Implement automated time
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2116:
RiskId: 723

ComplianceId: 735
RiskTitle: Unauthorized Access to Audit Information
Criticality: High
PossibleDamage: Data manipulation, deletion, or unauthorized changes to audit logs.
Category: Operational
RiskType: Current
BusinessImpact: Loss of data integrity, compromised compliance, and security posture.
RiskDescription: Unauthorized access to audit information could lead to falsification of records, hinderi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls for audit information", "2": "Regularly monitor acc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2117:
RiskId: 724
ComplianceId: 736
RiskTitle: Delay in Unauthorized Access Detection
Criticality: Medium
PossibleDamage: Extended exposure to unauthorized access incidents leading to data breaches or sy
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of data breaches and compromised system integrity.
RiskDescription: Failure to promptly detect and respond to unauthorized access incidents could result i
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement real-time alerting mechanisms for unauthorized access", "2": "Establis
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2118:
RiskId: 725
ComplianceId: 737
RiskTitle: Unauthorized Access to Audit Logging Management
Criticality: High
PossibleDamage: Tampering with audit records, hindering audit activities, compromising audit integrity
Category: Operational
RiskType: Current
BusinessImpact: Disruption of audit processes, compromised audit reliability, regulatory non-complianc
RiskDescription: Unauthorized access to audit logging management could result in unauthorized modif
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and regular monitoring of audit logs", "2": "Imple
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2119:
RiskId: 726
ComplianceId: 738
RiskTitle: Non-compliance with Audit Record Retention Requirements
Criticality: High
PossibleDamage: Regulatory fines, legal actions, compromised investigations

Category: Compliance
RiskType: Current
BusinessImpact: All business units within the organization may face penalties and legal consequences
RiskDescription: Failure to retain audit records for the required period may result in non-compliance wi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated retention policies and procedures", "2": "Regularly review a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2120:
RiskId: 727
ComplianceId: 739
RiskTitle: Failure to Generate Audit Records
Criticality: High
PossibleDamage: Undetected security incidents or compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, reputational damage, legal consequences
RiskDescription: Failure to generate audit records for all relevant event types may result in undetected
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the list of event types to be audited", "2": "Implemen
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2121:
RiskId: 728
ComplianceId: 740
RiskTitle: Unauthorized Event Type Selection
Criticality: Medium
PossibleDamage: Incomplete or inaccurate audit records
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches, regulatory non-compliance
RiskDescription: Unauthorized personnel selecting event types for logging may result in incomplete or
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement role-based access control for event type selection", "2": "Provide traini
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2122:
RiskId: 729
ComplianceId: 741
RiskTitle: Incomplete Audit Record Content
Criticality: High
PossibleDamage: Hindered incident response and compliance investigations
Category: Operational
RiskType: Current
BusinessImpact: Delayed incident response, compromised compliance investigations
RiskDescription: Incomplete or inaccurate audit record content may hinder incident response efforts ar

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review audit record content for compliance with AU-3", "2": "Implement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2123:
RiskId: 730
ComplianceId: 742
RiskTitle: Non-compliance with Assessment, Authorization, and Monitoring Policy
Criticality: High
PossibleDamage: Legal penalties, data breaches, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation, loss of customer trust
RiskDescription: Failure to comply with policy requirements may lead to unauthorized access to sensiti
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Employee training on policy implement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2124:
RiskId: 731

ComplianceId: 743
RiskTitle: Lack of Designated Official for Policy Management
Criticality: Medium
PossibleDamage: Inconsistent policy implementation, lack of oversight
Category: Operational
RiskType: Current
BusinessImpact: Operational inefficiencies, compliance gaps, increased risk of non-compliance
RiskDescription: Without a designated official, there may be confusion regarding policy ownership, lea
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear assignment of responsibilities and authority", "2": "Regular monitoring and r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2125:
RiskId: 732
ComplianceId: 744
RiskTitle: Outdated Policy and Procedures
Criticality: High
PossibleDamage: Non-compliance, security incidents, inefficiencies
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, increased risk exposure, potential legal consequences
RiskDescription: Failure to regularly review and update policies and procedures may result in non-com
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear review schedules and responsibilities", "2": "Regular training on pc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2126:
RiskId: 733
ComplianceId: 748
RiskTitle: Inaccurate Control Assessments
Criticality: High
PossibleDamage: Ineffective control measures and increased security risks
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential breaches, data loss, financial losses
RiskDescription: Failure to employ independent assessors may result in biased assessments that do n
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict guidelines for assessor independence", "2": "Conduct regular auc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2127:
RiskId: 734
ComplianceId: 749
RiskTitle: Inaccurate External Assessment Results
Criticality: High
PossibleDamage: Undetected security vulnerabilities

Category: Operational
RiskType: Current
BusinessImpact: Potential compromise of organizational systems and data
RiskDescription: Failure to accurately assess external control assessment results may result in undete
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhance due diligence in assessing external assessment providers", "2": "Implem
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2128:
RiskId: 735
ComplianceId: 750
RiskTitle: Unreliable Assessment Results for Cryptographic Modules
Criticality: Medium
PossibleDamage: Inaccurate security evaluations of cryptographic modules
Category: IT
RiskType: Current
BusinessImpact: Potential security vulnerabilities in cryptographic modules
RiskDescription: Failure to leverage accredited testing laboratories may result in unreliable assessmen
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear criteria for selecting accredited testing laboratories", "2": "Impleme
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2129:
RiskId: 736
ComplianceId: 751
RiskTitle: Failure to Develop Plan of Action and Milestones
Criticality: High
PossibleDamage: Increased vulnerability to cyber attacks, data breaches, and non-compliance penalti
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential security breaches and non-compli
RiskDescription: Failure to develop a plan of action and milestones may result in unresolved vulnerabil
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the plan of action and milestones", "2": "Allocate res
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2130:
RiskId: 737
ComplianceId: 752
RiskTitle: Failure to Update Plan of Action and Milestones
Criticality: Medium
PossibleDamage: Ineffective remediation strategies and increased vulnerability to new threats
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by ineffective remediation strategies and increa
RiskDescription: Failure to update the plan of action and milestones may result in outdated remediation

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update the plan based on assessment findings", "2": "Imple
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2131:
RiskId: 738
ComplianceId: 753
RiskTitle: Unauthorized System Operations
Criticality: High
PossibleDamage: Increased security risks and potential data breaches
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, damage to reputation
RiskDescription: Unauthorized system operations can lead to security breaches and compromise sens
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls and monitoring tools", "2": "Regularly review and upda
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2132:
RiskId: 739

ComplianceId: 754
RiskTitle: Inadequate Security Measures
Criticality: Medium
PossibleDamage: Increased vulnerabilities and potential data breaches
Category: IT
RiskType: Current
BusinessImpact: Loss of sensitive data, financial losses
RiskDescription: Failure to accept common controls may lead to inadequate security measures and inc
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly assess and update common controls", "2": "Implement multi-factor auth
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2133:
RiskId: 740
ComplianceId: 755
RiskTitle: Misaligned Security Controls
Criticality: Low
PossibleDamage: Increased security risks and potential compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Operational disruptions, potential data breaches
RiskDescription: Outdated authorizations may lead to misaligned security controls and increased secu
RiskLikelihood: 5
RiskImpact: 4
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Low
RiskMitigation: {"1": "Implement automated authorization update tools", "2": "Regularly review and upda
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2134:
RiskId: 741
ComplianceId: 756
RiskTitle: Ineffective system-level continuous monitoring
Criticality: High
PossibleDamage: Increased vulnerability to security threats, potential data breaches, and ineffective ris
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential security breaches and data leaks
RiskDescription: Failure to develop and implement an effective system-level continuous monitoring stra
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on continuous monitoring procedures",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2135:
RiskId: 742
ComplianceId: 757
RiskTitle: Undefined system-level metrics for continuous monitoring
Criticality: Medium
PossibleDamage: Ineffective monitoring and risk assessment due to lack of relevant system-level metr

Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by inaccurate risk assessments and ineffective
RiskDescription: Failure to establish specific system-level metrics for continuous monitoring may result
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review and update of system-level metrics based on changing threats an
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2136:
RiskId: 743
ComplianceId: 758
RiskTitle: Biased Assessments
Criticality: High
PossibleDamage: Inaccurate monitoring of controls and increased risk of control failures
Category: Compliance
RiskType: Inherent
BusinessImpact: All business units may be impacted by control failures
RiskDescription: Assessors with conflicts of interest may provide biased assessments, leading to inacc
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a formal process to verify the independence of assessors", "2": "Rotate
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2137:
RiskId: 744
ComplianceId: 759
RiskTitle: Ineffective Risk Monitoring
Criticality: High
PossibleDamage: Potential data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be affected by security and privacy risks
RiskDescription: Failure to implement effective risk monitoring may lead to undetected vulnerabilities, c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on risk monitoring procedures", "2": "A
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2138:
RiskId: 745
ComplianceId: 760
RiskTitle: Data Breach due to Undetected Vulnerabilities in Critical Systems
Criticality: High
PossibleDamage: Data breach resulting in financial losses, reputational damage, and legal consequen
Category: IT
RiskType: Current
BusinessImpact: Financial losses, reputational damage, legal consequences
RiskDescription: Failure to conduct annual penetration testing on critical systems may lead to undetect

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated vulnerability scanning tools", "2": "Engage experienced per
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2139:
RiskId: 746
ComplianceId: 761
RiskTitle: Unauthorized Exposure of Sensitive Information due to Lack of Rules of Engagement
Criticality: Medium
PossibleDamage: Legal implications, reputational damage, loss of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Legal implications, reputational damage
RiskDescription: Failure to establish clear rules of engagement for penetration testing may lead to una
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop comprehensive rules of engagement documents", "2": "Provide training c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2140:
RiskId: 747

ComplianceId: 762
RiskTitle: Biased or Ineffective Penetration Testing
Criticality: High
PossibleDamage: Undetected vulnerabilities, security breaches, financial losses
Category: IT
RiskType: Current
BusinessImpact: Financial losses, reputational damage, legal consequences
RiskDescription: Failure to employ independent penetration testing agents or teams may lead to biase
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and verify independence of penetration testing agents or teams"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2141:
RiskId: 748
ComplianceId: 763
RiskTitle: Unidentified Vulnerabilities from Lack of Red Team Exercises
Criticality: High
PossibleDamage: Data breaches, system compromises, loss of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation, legal implications
RiskDescription: Failure to conduct regular red team exercises may result in unidentified vulnerabilities
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Schedule regular red team exercises at least quarterly", "2": "Ensure red team ex
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2142:
RiskId: 749
ComplianceId: 764
RiskTitle: Unauthorized Internal Connections Risk
Criticality: High
PossibleDamage: Unauthorized internal connections may lead to data breaches, unauthorized access,
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential data breaches and unauthorized ac
RiskDescription: Unauthorized internal connections can result in unauthorized access to sensitive data
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and authentication mechanisms", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2143:
RiskId: 750
ComplianceId: 765
RiskTitle: Documentation of Internal Connections Risk
Criticality: Medium
PossibleDamage: Lack of documentation may lead to misconfiguration, security vulnerabilities, and no

Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by potential security vulnerabilities and non-com
RiskDescription: Inadequate documentation of internal connections can result in misconfiguration, secu
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement documentation standards and templates for internal connections", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2144:
RiskId: 751
ComplianceId: 766
RiskTitle: Review of Internal Connections Risk
Criticality: High
PossibleDamage: Failure to review internal connections may result in resource wastage, inefficiencies,
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by resource wastage and security risks
RiskDescription: Neglecting to review internal connections can lead to resource wastage, inefficiencies
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a review schedule for internal connections", "2": "Involve relevant stakel
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2145:
RiskId: 752
ComplianceId: 767
RiskTitle: Security Breach Due to Policy Non-Compliance
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal penalties
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, loss of customer trust, regulatory fines
RiskDescription: Failure to comply with the configuration management policy may result in unauthorize
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Employee training on policy requireme
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2146:
RiskId: 753
ComplianceId: 768
RiskTitle: Policy Oversight Failure
Criticality: Medium
PossibleDamage: Inconsistent policy enforcement, misalignment with regulations, increased security ri
Category: Operational
RiskType: Current
BusinessImpact: Confusion in policy implementation, increased vulnerability to security threats
RiskDescription: Failure to designate an official to manage configuration management policy may resu

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clear definition of official's responsibilities", "2": "Regular performance evaluations
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2147:
RiskId: 754
ComplianceId: 769
RiskTitle: Non-Compliance Due to Outdated Policies
Criticality: High
PossibleDamage: Regulatory fines, security breaches, operational inefficiencies
Category: Operational
RiskType: Current
BusinessImpact: Legal consequences, data breaches, disruption of operations
RiskDescription: Failure to review and update configuration management policies and procedures may
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish regular review schedules", "2": "Conduct thorough policy assessments",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2148:
RiskId: 755

ComplianceId: 770
RiskTitle: Unauthorized System Changes
Criticality: High
PossibleDamage: Security vulnerabilities, data breaches, operational disruptions
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial losses, reputational damage
RiskDescription: Unauthorized changes to system configurations can lead to security vulnerabilities an
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict change control procedures", "2": "Regularly review and update ba
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2149:
RiskId: 756
ComplianceId: 771
RiskTitle: Outdated Baseline Configurations
Criticality: Medium
PossibleDamage: Misconfigurations, security vulnerabilities, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Potential non-compliance penalties, data breaches, operational disruptions
RiskDescription: Outdated baseline configurations may lead to misconfigurations, security vulnerabilitie
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Automate configuration updates where possible", "2": "Regularly review and upda
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2150:
RiskId: 757
ComplianceId: 773
RiskTitle: Loss of Critical System Configurations
Criticality: High
PossibleDamage: System downtime, data loss, or unauthorized changes
Category: Operational
RiskType: Inherent
BusinessImpact: Significant impact on operations and potential financial losses
RiskDescription: Failure to retain previous baseline configurations may lead to system instability, unaut
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular backups of baseline configurations", "2": "Automated version control syst
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2151:
RiskId: 758
ComplianceId: 774
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, loss of intellectual property, reputational damage

Category: IT
RiskType: Inherent
BusinessImpact: Disruption of operations, financial losses, legal implications
RiskDescription: Unauthorized access to sensitive information stored on systems used in high-risk area
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls", "2": "Regularly monitor system activity for anom
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2152:
RiskId: 759
ComplianceId: 775
RiskTitle: Compromised Systems Upon Return from Travel
Criticality: Medium
PossibleDamage: Data breaches, loss of sensitive information, financial losses
Category: IT
RiskType: Inherent
BusinessImpact: Disruption of operations, reputational damage, legal implications
RiskDescription: Failure to apply controls to systems or components upon return from travel can result
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement endpoint security solutions", "2": "Regularly audit system configuration
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2153:
RiskId: 760
ComplianceId: 776
RiskTitle: Failure to Document Configuration Changes
Criticality: High
PossibleDamage: Audit failures, security breaches, unauthorized system modifications
Category: Operational
RiskType: Current
BusinessImpact: Potential impact on system integrity, data confidentiality, and regulatory compliance
RiskDescription: Failure to document configuration changes may result in unauthorized modifications, s
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a centralized system for documenting and storing configuration-contro
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2154:
RiskId: 761
ComplianceId: 777
RiskTitle: Failure to Review and Approve Changes
Criticality: High
PossibleDamage: Security vulnerabilities, privacy breaches, system instability
Category: Operational
RiskType: Current
BusinessImpact: Potential impact on system security, data privacy, and operational stability
RiskDescription: Failure to review and approve changes may lead to unauthorized system modification

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a formal review process with security and privacy impact analyses", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2155:
RiskId: 762
ComplianceId: 778
RiskTitle: System Downtime Due to Unvalidated Changes
Criticality: High
PossibleDamage: Loss of productivity, revenue, and customer trust
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of business operations and financial losses
RiskDescription: Failure to validate system changes may lead to unexpected system downtime and op
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a comprehensive testing protocol", "2": "Implement change control proc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2156:
RiskId: 763

ComplianceId: 779
RiskTitle: Unauthorized Configuration Changes
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, non-compliance penalties
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties, reputational damage
RiskDescription: Unauthorized changes to system configurations can lead to security vulnerabilities, da
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls for configuration change approvals", "2": "Regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2157:
RiskId: 764
ComplianceId: 780
RiskTitle: Failure to Conduct Impact Analyses Before System Changes
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, privacy breaches, regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, financial losses, damage to reputation
RiskDescription: Failure to conduct impact analyses before system changes may lead to unidentified s
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear impact analysis procedures", "2": "Train personnel on conducting i
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2158:
RiskId: 765
ComplianceId: 781
RiskTitle: Security Breach Due to Unverified Controls
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, regulatory fines
RiskDescription: Failure to verify controls post system changes may lead to vulnerabilities being exploi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Encrypt sensitive data at rest and in t
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2159:
RiskId: 766
ComplianceId: 782
RiskTitle: Unauthorized Changes Risk
Criticality: High
PossibleDamage: System downtime, data breaches, privacy violations

Category: Operational
RiskType: Current
BusinessImpact: Potential loss of sensitive data, disruption of operations
RiskDescription: Unauthorized changes by unqualified personnel can compromise system integrity and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access control", "2": "Enforce multi-factor authentication for
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2160:
RiskId: 767
ComplianceId: 783
RiskTitle: Unplanned Changes Risk
Criticality: Medium
PossibleDamage: System instability, downtime, operational issues
Category: Operational
RiskType: Current
BusinessImpact: Disruption of regular operations, potential financial losses
RiskDescription: Changes made outside of designated windows can disrupt critical processes and lead
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear change windows and communicate them to all stakeholders", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2161:
RiskId: 768
ComplianceId: 784
RiskTitle: Unauthorized Configuration Changes
Criticality: High
PossibleDamage: System vulnerabilities, data breaches, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, reputation damage, financial losses
RiskDescription: Unauthorized changes can compromise system integrity and confidentiality, leading to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict change control processes", "2": "Regularly audit access logs", "3"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2162:
RiskId: 769
ComplianceId: 785
RiskTitle: Lack of Audit Records
Criticality: Medium
PossibleDamage: Inability to trace unauthorized changes, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Loss of accountability, regulatory fines, reputation damage
RiskDescription: Without audit records, organizations cannot verify the integrity of configuration change

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement robust logging mechanisms", "2": "Regularly review audit logs", "3": "C
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2163:
RiskId: 770
ComplianceId: 786
RiskTitle: Unauthorized Changes to Production Systems
Criticality: High
PossibleDamage: Disruption of critical business operations, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Potential system downtime, data loss, financial impact
RiskDescription: Unauthorized changes to production systems could lead to system instability, data co
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access control", "2": "Implement regular access reviews", "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2164:
RiskId: 771

ComplianceId: 787
RiskTitle: Outdated Privileges for System Changes
Criticality: Medium
PossibleDamage: Security breaches, unauthorized system changes
Category: IT
RiskType: Residual
BusinessImpact: Data breaches, compliance violations
RiskDescription: Outdated or unnecessary privileges for system changes could lead to unauthorized ac
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement regular access reviews", "2": "Automate privilege review process", "3":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2165:
RiskId: 772
ComplianceId: 788
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breach, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of customer trust and financial penalties
RiskDescription: Unauthorized access to system components due to insecure configuration settings co
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implementing multi-factor authentication", "2": "Regular security training for emplo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2166:
RiskId: 773
ComplianceId: 789
RiskTitle: Vulnerability Risk
Criticality: Medium
PossibleDamage: System vulnerabilities, potential data breaches
Category: IT
RiskType: Residual
BusinessImpact: Loss of data integrity, system downtime
RiskDescription: Failure to implement approved configuration settings could lead to system vulnerabilit
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular vulnerability scanning", "2": "Patch management process", "3": "Continuo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2167:
RiskId: 774
ComplianceId: 790
RiskTitle: Data Breach due to Misconfigured Settings
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage

Category: IT
RiskType: Residual
BusinessImpact: Significant financial and reputational damage
RiskDescription: Misconfigured settings could allow unauthorized access to sensitive data, leading to a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Encrypt sensitive data at rest and in t
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2168:
RiskId: 775
ComplianceId: 791
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, system compromise, loss of sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of data, reputation damage, financial losses
RiskDescription: Unauthorized access to non-essential functions can lead to exploitation of system vul
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls", "2": "Regularly review and update access per
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2169:
RiskId: 776
ComplianceId: 792
RiskTitle: Prohibited Functions Risk
Criticality: Medium
PossibleDamage: System vulnerabilities, exploitation, unauthorized access
Category: Operational
RiskType: Current
BusinessImpact: Potential security breaches, data loss, reputation damage
RiskDescription: Unauthorized use of prohibited functions and services can lead to system vulnerabiliti
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update and enforce the list of prohibited functions and services", "2": "Ir
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2170:
RiskId: 777
ComplianceId: 793
RiskTitle: Security Vulnerabilities Due to Unnecessary Functions
Criticality: High
PossibleDamage: Exposure to security vulnerabilities and potential unauthorized access to systems
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial losses, damage to reputation
RiskDescription: Unnecessary functions and services may introduce security vulnerabilities that could l

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular vulnerability scanning and patch management", "2": "Implementing netwo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2171:
RiskId: 778
ComplianceId: 794
RiskTitle: Data Breach Due to Unauthorized Program Execution
Criticality: High
PossibleDamage: Data loss, financial penalties, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Significant financial and reputational damage
RiskDescription: Unauthorized execution of malicious software could lead to a data breach resulting in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular software updates and patches", "2": "Network segmentation to contain br
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2172:
RiskId: 779

ComplianceId: 795
RiskTitle: Compliance Violation Due to Unauthorized Program Execution
Criticality: Medium
PossibleDamage: Legal penalties, reputational damage, operational disruptions
Category: Operational
RiskType: Residual
BusinessImpact: Operational delays and potential legal consequences
RiskDescription: Unauthorized program execution by unauthorized roles could lead to compliance viola
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular access reviews and updates", "2": "Automated approval workflows", "3": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2173:
RiskId: 780
ComplianceId: 796
RiskTitle: Unauthorized Software Execution Risk
Criticality: High
PossibleDamage: Unauthorized software execution may lead to security breaches and data loss.
Category: IT
RiskType: Current
BusinessImpact: All business units would be impacted by potential security breaches and data loss
RiskDescription: Unauthorized software execution poses a significant risk to the organization's security
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the list of authorized software programs", "2": "Imple
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2174:
RiskId: 781
ComplianceId: 797
RiskTitle: Policy Mismanagement Risk
Criticality: Medium
PossibleDamage: Failure to implement the policy may result in unauthorized software execution and s
Category: IT
RiskType: Current
BusinessImpact: All business units would be impacted by potential security breaches and data loss
RiskDescription: Failure to implement the deny-all, permit-by-exception policy may lead to unauthorize
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update the list of authorized software programs", "2": "Imple
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2175:
RiskId: 782
ComplianceId: 798
RiskTitle: Inaccurate tracking of system components
Criticality: High
PossibleDamage: Security breaches, compliance violations, and operational disruptions

Category: Operational
RiskType: Current
BusinessImpact: All business units would be affected by the potential consequences of inaccurate trac
RiskDescription: Failure to accurately track system components can lead to unauthorized access, data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of the system component inventory to identify and correct any disc
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2176:
RiskId: 783
ComplianceId: 799
RiskTitle: Outdated system component inventory
Criticality: Medium
PossibleDamage: Inaccurate reporting, security vulnerabilities, and compliance issues
Category: Operational
RiskType: Current
BusinessImpact: All business units would be affected by the potential consequences of an outdated sy
RiskDescription: An outdated inventory can lead to misinformed decision-making, security vulnerabilitie
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a regular schedule for inventory reviews and updates", "2": "Automate in
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2177:
RiskId: 784
ComplianceId: 800
RiskTitle: Security Vulnerabilities Due to Incomplete Inventory
Criticality: High
PossibleDamage: Security breaches, data loss, system downtime
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Incomplete system component inventories may lead to unidentified vulnerabilities that
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security scans and audits", "2": "Implementing access controls and monit
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2178:
RiskId: 785
ComplianceId: 801
RiskTitle: Security Breach Due to Unauthorized Components
Criticality: High
PossibleDamage: Unauthorized access to sensitive data, system downtime, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of data, financial implications, regulatory fines
RiskDescription: Unauthorized components could provide entry points for malicious actors to exploit vu

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular automated scans for unauthorized components", "2": "Immediate isolatio
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2179:
RiskId: 786
ComplianceId: 802
RiskTitle: Inadequate Configuration Management Plan
Criticality: High
PossibleDamage: Failure to manage system configurations effectively leading to security breaches an
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of operations, loss of sensitive data, and reputational damage
RiskDescription: The absence of a well-defined configuration management plan increases the risk of u
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of system configurations", "2": "Implement automated configuratio
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2180:
RiskId: 787

ComplianceId: 803
RiskTitle: Unapproved Configuration Management Plan
Criticality: Medium
PossibleDamage: Implementation of outdated or inaccurate configuration management processes lead
Category: Operational
RiskType: Inherent
BusinessImpact: Project delays, increased costs, and reduced system reliability
RiskDescription: Lack of approval for the configuration management plan may result in the use of outd
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a formal approval workflow for configuration management plans", "2": "C
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2181:
RiskId: 788
ComplianceId: 804
RiskTitle: Copyright Infringement Risk
Criticality: High
PossibleDamage: Legal penalties, fines, and reputational damage
Category: Legal
RiskType: Inherent
BusinessImpact: Potential legal costs and damage to reputation.
RiskDescription: Unauthorized use of software can lead to copyright infringement claims and legal acti
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training on software usage policies and copyright laws", "2": "Implement s
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2182:
RiskId: 789
ComplianceId: 805
RiskTitle: Unauthorized Distribution Risk
Criticality: Medium
PossibleDamage: Financial losses
Category: Financial
RiskType: Inherent
BusinessImpact: Financial losses due to unauthorized distribution of software.
RiskDescription: Unauthorized copying and distribution of software with quantity licenses can lead to fi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement software usage monitoring tools", "2": "Regular audits of software usag
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2183:
RiskId: 790
ComplianceId: 806
RiskTitle: Unauthorized File Sharing Risk
Criticality: High
PossibleDamage: Legal liabilities

Category: Legal
RiskType: Inherent
BusinessImpact: Legal liabilities due to unauthorized sharing of copyrighted work.
RiskDescription: Unauthorized use of peer-to-peer file sharing technology can lead to legal liabilities fo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Block peer-to-peer file sharing technology on company devices", "2": "Monitor net
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2184:
RiskId: 791
ComplianceId: 807
RiskTitle: Risk of Unauthorized Software Installations
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats, potential data breaches, and system instabil
Category: IT
RiskType: Inherent
BusinessImpact: All business units would be impacted by potential data breaches and system instabilit
RiskDescription: Unauthorized software installations can introduce malware, spyware, or other maliciou
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and enforce software installation policies", "2": "Provide training
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2185:
RiskId: 792
ComplianceId: 808
RiskTitle: Risk of Inadequate Enforcement of Software Installation Policies
Criticality: Medium
PossibleDamage: Increased vulnerability to cyber threats, potential data breaches, and system instabil
Category: IT
RiskType: Inherent
BusinessImpact: All business units would be impacted by potential data breaches and system instabilit
RiskDescription: Failure to enforce software installation policies can result in unauthorized software ins
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated monitoring tools to detect unauthorized software installatio
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2186:
RiskId: 793
ComplianceId: 809
RiskTitle: Data Breach Due to Unidentified Information Location
Criticality: High
PossibleDamage: Financial loss, reputational damage, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Significant financial and reputational damage
RiskDescription: Failure to identify and document information location may lead to unauthorized acces

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls and encryption mechanisms", "2": "Regularly monitor a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2187:
RiskId: 794
ComplianceId: 810
RiskTitle: Unauthorized Access to Information Location
Criticality: Medium
PossibleDamage: Data leaks, compliance violations
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations and potential legal consequences
RiskDescription: Failure to document user access may result in unauthorized access and misuse of se
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement role-based access controls", "2": "Regularly review and update user ac
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2188:
RiskId: 795

ComplianceId: 811
RiskTitle: Data Loss Due to Unmanaged Information Location Changes
Criticality: Low
PossibleDamage: Data loss, system disruptions
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions and potential data loss
RiskDescription: Failure to document and manage changes to information location may result in data lo
RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Implement change management processes", "2": "Conduct impact assessments b
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2189:
RiskId: 796
ComplianceId: 812
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data exposure, financial losses, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Unauthorized access to sensitive information due to inadequate automated tools usag
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular security audits and penetration testing", "2": "Implementing multi-factor a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2190:
RiskId: 797
ComplianceId: 813
RiskTitle: Inadequate Contingency Planning Policy
Criticality: High
PossibleDamage: Financial losses, reputational damage, and operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Disruptions in operations, financial losses, and reputational damage
RiskDescription: Failure to have a clear and comprehensive contingency planning policy may result in
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates to ensure alignment with current regulations"
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2191:
RiskId: 798
ComplianceId: 814
RiskTitle: Lack of Designated Official for Policy Management
Criticality: Medium
PossibleDamage: Confusion, delays, or inconsistencies in policy management

Category: Operational
RiskType: Current
BusinessImpact: Policy management and implementation processes may be affected
RiskDescription: Failure to designate an official to manage the contingency planning policy and proced
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clearly define roles and responsibilities of the designated official", "2": "Regular c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2192:
RiskId: 799
ComplianceId: 815
RiskTitle: Outdated Contingency Planning Policy and Procedures
Criticality: High
PossibleDamage: Ineffective response to emergencies or disruptions
Category: Operational
RiskType: Current
BusinessImpact: All business units may be impacted by ineffective response to emergencies or disrupt
RiskDescription: Failure to review and update the contingency planning policy and procedures may lea
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy and procedure reviews to identify gaps and updates", "2": "Training
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2193:
RiskId: 800
ComplianceId: 816
RiskTitle: Failure to Develop Contingency Plan
Criticality: High
PossibleDamage: Prolonged system downtime, loss of critical data, inability to restore essential functio
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Failure to develop a contingency plan may result in significant operational disruptions
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the contingency plan", "2": "Conduct contingency pla
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2194:
RiskId: 801
ComplianceId: 817
RiskTitle: Lack of Coordination in Contingency Planning
Criticality: Medium
PossibleDamage: Delays in activating contingency plans, extended system downtime, increased impac
Category: Operational
RiskType: Current
BusinessImpact: All business units
RiskDescription: Lack of coordination between contingency planning and incident handling teams may

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels between contingency planning and incid
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2195:
RiskId: 802
ComplianceId: 818
RiskTitle: Disjointed Response Efforts
Criticality: High
PossibleDamage: Increased downtime, financial losses, and reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Delays in response and recovery efforts
RiskDescription: Failure to coordinate contingency plan development with related plans may lead to dis
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication channels between teams responsible for different
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2196:
RiskId: 803

ComplianceId: 819
RiskTitle: Failure to Resume Essential Functions
Criticality: High
PossibleDamage: Extended downtime, loss of revenue, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Inability to resume essential functions within the defined time period could result in sig
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and updating of contingency plans", "2": "Training employees on c
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2197:
RiskId: 804
ComplianceId: 820
RiskTitle: Unauthorized Access to Critical Assets
Criticality: High
PossibleDamage: Loss of sensitive data, disruption of business operations
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of critical business functions and potential financial losses
RiskDescription: Unauthorized access to critical assets can lead to data breaches, system downtime, a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls and authentication mechanisms", "2": "Regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2198:
RiskId: 805
ComplianceId: 821
RiskTitle: Inadequate Contingency Training for System Users
Criticality: High
PossibleDamage: Confusion, errors, and delays during contingency operations
Category: Operational
RiskType: Current
BusinessImpact: Delays or errors in response during contingency operations
RiskDescription: Failure to provide adequate contingency training to system users may result in confus
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update training content to align with current roles and respo
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2199:
RiskId: 806
ComplianceId: 822
RiskTitle: Ineffective Contingency Response
Criticality: High
PossibleDamage: Operational disruptions, financial losses, reputational damage

Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, reputational damage, customer dissatisfaction
RiskDescription: Failure to test contingency plans may result in inadequate response during emergenc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and training of staff", "2": "Review and update contingency plans b
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2200:
RiskId: 807
ComplianceId: 823
RiskTitle: Missed Opportunities for Improvement
Criticality: Medium
PossibleDamage: Ineffective contingency plans, compromised operational response
Category: Operational
RiskType: Inherent
BusinessImpact: Operational disruptions, potential financial losses
RiskDescription: Failure to review contingency plan test results may result in missed opportunities for i
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a review committee to analyze test results", "2": "Implement a feedback
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2201:
RiskId: 808
ComplianceId: 824
RiskTitle: Ineffective Coordination of Contingency Plan Testing
Criticality: High
PossibleDamage: Extended downtime, financial losses, and reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, and damage to organizational reputation
RiskDescription: Failure to coordinate contingency plan testing with related plans may lead to confusio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear communication channels and protocols for coordination", "2": "Reg
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2202:
RiskId: 809
ComplianceId: 825
RiskTitle: Data Loss Due to Primary Storage Site Failure
Criticality: High
PossibleDamage: Loss of critical data and information
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of business operations, potential financial losses
RiskDescription: Failure to establish an alternate storage site may result in the loss of critical data and

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing of backup retrieval process", "2": "Periodic review and update of a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2203:
RiskId: 810
ComplianceId: 826
RiskTitle: Data Breach Due to Inadequate Security Controls at Alternate Storage Site
Criticality: Medium
PossibleDamage: Data breach or unauthorized access
Category: Operational
RiskType: Inherent
BusinessImpact: Loss of sensitive data, reputation damage
RiskDescription: Failure to ensure equivalent security controls at the alternate storage site may result i
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular security audits and assessments at the alternate storage site", "2": "Imple
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2204:
RiskId: 811

ComplianceId: 827
RiskTitle: Data Loss and Operational Disruption
Criticality: High
PossibleDamage: Loss of critical data, operational disruptions, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Significant impact on business operations and reputation
RiskDescription: Failure to comply with the separation requirement may lead to data loss and operation
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and monitoring of security measures", "2": "Implementing redunda
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2205:
RiskId: 812
ComplianceId: 828
RiskTitle: Alternate Storage Site Accessibility Failure
Criticality: High
PossibleDamage: Loss of critical data, disruption of business operations
Category: Operational
RiskType: Current
BusinessImpact: IT, Data Management
RiskDescription: Failure to access alternate storage site during a disaster may result in prolonged dow
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular testing of alternate site accessibility", "2": "Establishing communication pr
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2206:
RiskId: 813
ComplianceId: 829
RiskTitle: Failure of Alternate Processing Site
Criticality: High
PossibleDamage: Disruption of essential mission and business functions, financial losses, reputational
Category: Operational
RiskType: Current
BusinessImpact: Disruption of essential functions and potential financial losses
RiskDescription: If the alternate processing site fails to transfer and resume operations effectively, the
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and validation of alternate processing site capabilities", "2": "Perio
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2207:
RiskId: 814
ComplianceId: 830
RiskTitle: Equipment and Supplies Shortage at Alternate Processing Site
Criticality: Medium
PossibleDamage: Delay in transfer and resumption of operations, increased downtime, financial losses

Category: Operational
RiskType: Current
BusinessImpact: Delays in operations resumption and potential financial losses
RiskDescription: If the necessary equipment and supplies are not available at the alternate processing
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular inventory checks and replenishment of equipment and supplies at the alt
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2208:
RiskId: 815
ComplianceId: 831
RiskTitle: Inadequate Controls at Alternate Processing Site
Criticality: High
PossibleDamage: Security breaches, data loss, operational disruptions
Category: Operational
RiskType: Current
BusinessImpact: Security breaches and operational disruptions
RiskDescription: If the controls at the alternate processing site are not equivalent to those at the prima
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits and assessments of controls at the alternate processing site", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2209:
RiskId: 816
ComplianceId: 832
RiskTitle: Lack of Alternate Processing Site
Criticality: High
PossibleDamage: Prolonged downtime, data loss, and financial losses
Category: Operational
RiskType: Inherent
BusinessImpact: All business units within the organization
RiskDescription: Failure to identify an alternate processing site may result in the inability to continue op
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and failover drills to ensure the alternate site is functional", "2": "In
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2210:
RiskId: 817
ComplianceId: 833
RiskTitle: Inaccessibility to Alternate Processing Sites
Criticality: High
PossibleDamage: Loss of critical business functions and data accessibility
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption to business operations and potential financial losses
RiskDescription: Inability to access alternate processing sites during disasters can result in significant d

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular accessibility assessments", "2": "Implementing accessibility improvement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2211:
RiskId: 818
ComplianceId: 834
RiskTitle: Inadequate Accessibility Measures at Alternate Processing Sites
Criticality: Medium
PossibleDamage: Operational disruptions and data unavailability
Category: Operational
RiskType: Inherent
BusinessImpact: Extended recovery times and potential data loss
RiskDescription: Lack of proper accessibility measures at alternate processing sites can lead to delays
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing accessibility protocols", "2": "Regularly testing accessibility measures
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2212:
RiskId: 819

ComplianceId: 835
RiskTitle: Failure to Prioritize Processing Needs at Alternate Site
Criticality: High
PossibleDamage: Extended downtime, data loss, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption to critical operations, financial losses, customer dissatisfaction
RiskDescription: In the event of a disaster, service providers may not prioritize the organization's proce
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update agreements with service providers", "2": "Conduct p
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2213:
RiskId: 820
ComplianceId: 836
RiskTitle: Failure of Alternate Telecommunications Services
Criticality: High
PossibleDamage: Disruption of essential mission and business functions, financial losses, reputational
Category: Operational
RiskType: Current
BusinessImpact: Loss of critical communication channels, delays in decision-making processes, inabili
RiskDescription: The risk of failure of alternate telecommunications services could lead to significant di
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular testing and maintenance of alternate telecommunications services", "2": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2214:
RiskId: 821
ComplianceId: 837
RiskTitle: Delayed Service Restoration
Criticality: High
PossibleDamage: Critical communication failures during emergencies
Category: Operational
RiskType: Residual
BusinessImpact: Disruption in critical communication channels
RiskDescription: Failure to prioritize service provisions in agreements could result in delayed service re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update service agreements", "2": "Conduct regular testing o
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2215:
RiskId: 822
ComplianceId: 838
RiskTitle: Lack of Priority Access
Criticality: High
PossibleDamage: Hindrance in critical national security communications during emergencies

Category: Operational
RiskType: Residual
BusinessImpact: Compromised national security communications
RiskDescription: Failure to request Telecommunications Service Priority could result in lack of priority a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly verify TSP enrollment status", "2": "Establish communication protocols v
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2216:
RiskId: 823
ComplianceId: 839
RiskTitle: Single Point of Failure in Telecommunications Services
Criticality: High
PossibleDamage: Service disruption, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of critical communications, impact on customer service, potential revenue l
RiskDescription: Failure of primary telecommunications services due to shared physical lines leading to
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement redundant telecommunications services from different providers", "2": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2217:
RiskId: 824
ComplianceId: 840
RiskTitle: Backup Frequency Risk
Criticality: High
PossibleDamage: Loss of critical data, compromised system integrity
Category: Operational
RiskType: Current
BusinessImpact: IT operations disruption, potential data breaches
RiskDescription: Failure to conduct backups at defined frequencies may result in data loss, system dow
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated backup scheduling tools", "2": "Regularly test backup resto
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2218:
RiskId: 825
ComplianceId: 841
RiskTitle: Backup Information Protection Risk
Criticality: High
PossibleDamage: Unauthorized access to backup data, data tampering, loss of data integrity
Category: Operational
RiskType: Current
BusinessImpact: Data breach, compromised data integrity
RiskDescription: Failure to protect backup information may result in unauthorized access, data tamperi

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls and encryption for backup storage", "2": "Regularly au
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2219:
RiskId: 826
ComplianceId: 842
RiskTitle: Backup Information Testing Failure
Criticality: High
PossibleDamage: Loss of critical data, compromised system integrity
Category: IT
RiskType: Current
BusinessImpact: Disruption of operations, potential data breaches
RiskDescription: Failure to test backup information could result in the inability to retrieve critical data or
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular testing and monitoring of backup systems", "2": "Implementing encryption
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2220:
RiskId: 827

ComplianceId: 843
RiskTitle: Data Breach Due to Inadequate Cryptographic Protection
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage, legal consequences
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, legal liabilities
RiskDescription: Inadequate cryptographic protection may lead to unauthorized access to backup infor
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption algorithms for backup data", "2": "Enforce strict acce
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2221:
RiskId: 828
ComplianceId: 844
RiskTitle: Extended System Downtime Risk
Criticality: High
PossibleDamage: Financial losses, reputational damage, operational disruptions
Category: Operational
RiskType: Residual
BusinessImpact: Extended system downtime can lead to loss of revenue, customer dissatisfaction, and
RiskDescription: Failure to meet recovery time objectives can result in prolonged system downtime and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular testing of recovery procedures", "2": "Implementing automated recovery
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2222:
RiskId: 829
ComplianceId: 845
RiskTitle: Data Loss and System Downtime
Criticality: High
PossibleDamage: Data loss, financial losses, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: IT, Operations
RiskDescription: Failure to implement transaction recovery mechanisms can result in data loss, system
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular backups of transaction logs", "2": "Testing of recovery mechanisms regul
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2223:
RiskId: 830
ComplianceId: 846
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information and data breaches

Category: IT
RiskType: Residual
BusinessImpact: All business units would be impacted by potential data breaches and unauthorized ac
RiskDescription: Unauthorized access to sensitive information due to lack of clear identification and au
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regular security audits", "3": "Continu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2224:
RiskId: 831
ComplianceId: 847
RiskTitle: Policy Oversight Risk
Criticality: Medium
PossibleDamage: Inconsistent policy implementation and oversight
Category: Operational
RiskType: Residual
BusinessImpact: All business units would be impacted by inconsistent policy implementation and overs
RiskDescription: Lack of designated official may lead to inconsistent policy implementation and oversig
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular policy audits", "2": "Training for designated official", "3": "Clear communic
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2225:
RiskId: 832
ComplianceId: 848
RiskTitle: Unauthorized Access to Organizational Systems
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information, reputational damage.
Category: Operational
RiskType: Current
BusinessImpact: Loss of confidential information, financial losses, legal consequences.
RiskDescription: Unauthorized access to organizational systems can lead to data breaches, loss of ser
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls and multi-factor authentication", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2226:
RiskId: 833
ComplianceId: 849
RiskTitle: Unauthorized Access to Privileged Accounts
Criticality: High
PossibleDamage: Data breaches, system compromise, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Potential disruption of operations, loss of sensitive data, financial liabilities
RiskDescription: Unauthorized access to privileged accounts can lead to unauthorized system changes

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update multi-factor authentication configurations", "2": "Impl
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2227:
RiskId: 834
ComplianceId: 850
RiskTitle: Unauthorized Access to Non-privileged Accounts
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, financial loss
Category: Operational
RiskType: Residual
BusinessImpact: Potential data breaches, financial loss, reputational damage
RiskDescription: Unauthorized access to non-privileged accounts can lead to exposure of sensitive info
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly monitor access logs for unusual activity", "2": "Implement real-time alert
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2228:
RiskId: 835

ComplianceId: 851
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Unauthorized users gaining access to sensitive data or resources, leading to data bre
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for all users", "2": "Regularly review and upd
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2229:
RiskId: 836
ComplianceId: 852
RiskTitle: Unauthorized Access to Privileged Accounts
Criticality: High
PossibleDamage: Potential data breaches and financial loss
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial penalties, damage to reputation
RiskDescription: Unauthorized access to privileged accounts can lead to data breaches, financial loss,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular security awareness training for users", "2": "Periodic review of access log
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2230:
RiskId: 837
ComplianceId: 853
RiskTitle: Unauthorized Access to Privileged Accounts
Criticality: High
PossibleDamage: Data breaches, financial loss, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive information, disruption of operations, financial liabilities
RiskDescription: Unauthorized individuals gaining access to privileged accounts can lead to unauthoriz
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for privileged accounts", "2": "Regularly upd
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2231:
RiskId: 838
ComplianceId: 854
RiskTitle: Unauthorized Access Due to Non-Verification of PIV-Compliant Credentials
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, potential data breaches, compromised

Category: Operational
RiskType: Current
BusinessImpact: Potential loss of sensitive data, financial losses, reputational damage
RiskDescription: Failure to accept and verify PIV-compliant credentials may lead to unauthorized acces
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for additional security layers", "2": "Regularl
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2232:
RiskId: 839
ComplianceId: 855
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of customer trust, financial implications
RiskDescription: Unauthorized devices gaining access to the network can lead to data breaches and c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement network segmentation to isolate devices", "2": "Regularly audit device
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2233:
RiskId: 840
ComplianceId: 856
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, compromised system
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, legal consequences, damage to reputation
RiskDescription: Unauthorized access to system resources due to improper identifier assignment
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly audit identifier assignments
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2234:
RiskId: 841
ComplianceId: 857
RiskTitle: Identifier Reuse Risk
Criticality: Medium
PossibleDamage: Confusion in system identification, potential security vulnerabilities, data integrity iss
Category: Operational
RiskType: Residual
BusinessImpact: Data integrity issues, system errors, compromised security
RiskDescription: Reuse of identifiers leading to misidentification, security vulnerabilities, and data integ

RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated identifier tracking systems", "2": "Enforce strict identifier reu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2235:
RiskId: 842
ComplianceId: 858
RiskTitle: Unauthorized Access Risk due to Unidentified Contractors
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches or leaks
RiskDescription: Failure to identify contractors may lead to unauthorized access to sensitive informatio
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular audits to verify contractor identification", "2": "Training for employees on i
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2236:
RiskId: 843

ComplianceId: 859
RiskTitle: Compliance Violation Risk due to Unidentified Foreign Nationals
Criticality: High
PossibleDamage: Regulatory fines or legal actions
Category: Legal
RiskType: Current
BusinessImpact: Potential legal consequences
RiskDescription: Failure to identify foreign nationals may lead to non-compliance with regulations and p
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verification of foreign national status through official documentation", "2": "Trainin
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2237:
RiskId: 844
ComplianceId: 860
RiskTitle: Unauthorized Access Due to Lack of Identity Verification
Criticality: High
PossibleDamage: Unauthorized access to sensitive systems and data
Category: Operational
RiskType: Residual
BusinessImpact: Potential data breaches, financial losses, and reputational damage
RiskDescription: Failure to verify the identity of individuals receiving authenticators can lead to unautho
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for additional verification", "2": "Regularly au
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2238:
RiskId: 845
ComplianceId: 861
RiskTitle: Unauthorized Access to Authenticator Content
Criticality: High
PossibleDamage: System compromise and data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Potential data breaches, financial losses, and reputational damage
RiskDescription: Unauthorized access to authenticator content can lead to compromised authentication
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for stored authenticator content", "2": "Enforce access contr
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2239:
RiskId: 846
ComplianceId: 862
RiskTitle: Weak Password Usage
Criticality: High
PossibleDamage: Increased risk of unauthorized access

Category: Operational
RiskType: Current
BusinessImpact: Unauthorized access to sensitive data
RiskDescription: Unauthorized users gaining access to sensitive information due to weak password us
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update the list of compromised passwords", "2": "Educate users on pas
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2240:
RiskId: 847
ComplianceId: 863
RiskTitle: Password Interception
Criticality: High
PossibleDamage: Unauthorized interception of passwords
Category: Operational
RiskType: Current
BusinessImpact: Unauthorized access to sensitive data
RiskDescription: Passwords being intercepted during transmission or storage leading to unauthorized a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Use secure communication protocols for password transmission", "2": "Regularly
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2241:
RiskId: 848
ComplianceId: 864
RiskTitle: Unauthorized Access to Private Keys
Criticality: High
PossibleDamage: Identity theft, data breaches, system compromise
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, reputational damage, financial losses
RiskDescription: Unauthorized access to private keys can lead to impersonation, data breaches, and c
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls and multi-factor authentication for private key a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2242:
RiskId: 849
ComplianceId: 865
RiskTitle: Invalid Certificate Validation
Criticality: High
PossibleDamage: Unauthorized access, data breaches, system compromise
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, reputational damage, financial losses
RiskDescription: Failure to validate certificates can lead to unauthorized access, data breaches, and co

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update trust anchors and revocation data in the cache", "2": "Implement
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2243:
RiskId: 850
ComplianceId: 866
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial repercussions, damage to reputation
RiskDescription: Unauthorized access to sensitive information due to inadequate protection of authenti
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for added security", "2": "Regularly review a
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2244:
RiskId: 851

ComplianceId: 867
RiskTitle: Data Breach Due to Unencrypted Authenticators
Criticality: High
PossibleDamage: Data breaches, financial loss, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of sensitive information, financial penalties, damage to reputation
RiskDescription: Unauthorized access to unencrypted authenticators could lead to a data breach, resu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Encrypt all static authenticators", "2": "Implement access controls and monitoring'
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2245:
RiskId: 852
ComplianceId: 868
RiskTitle: Unauthorized Access Risk due to Unobscured Authentication Feedback
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, compromised user accounts, data bre
Category: Operational
RiskType: Residual
BusinessImpact: Potential unauthorized access to sensitive data, compromised user accounts, data br
RiskDescription: Failure to obscure authentication feedback during the authentication process may lea
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement password masking by displaying asterisks when users type passwords
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2246:
RiskId: 853
ComplianceId: 869
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, compromised sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Loss of data integrity, confidentiality, and availability
RiskDescription: Unauthorized access to cryptographic modules can lead to data breaches, compromis
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly monitor access logs", "3": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2247:
RiskId: 854
ComplianceId: 870
RiskTitle: Vulnerability Detection Risk
Criticality: Medium
PossibleDamage: Security breaches, unauthorized access

Category: IT
RiskType: Residual
BusinessImpact: Disruption of services, loss of data integrity
RiskDescription: Undetected vulnerabilities in authentication mechanisms can lead to unauthorized acc
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular security audits", "2": "Implement intrusion detection systems", "3": "Enfor
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2248:
RiskId: 855
ComplianceId: 871
RiskTitle: Unauthorized Access to Federal Systems
Criticality: High
PossibleDamage: Data breaches, information leakage, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Unauthorized access by non-organizational users can lead to data breaches and com
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for all users", "2": "Regularly review access
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2249:
RiskId: 856
ComplianceId: 872
RiskTitle: Unauthorized Access to Sensitive Information
Criticality: High
PossibleDamage: Data breaches, compromised system integrity
Category: Operational
RiskType: Residual
BusinessImpact: Potential loss of sensitive data, financial losses, damage to reputation
RiskDescription: Unauthorized access to sensitive information due to inadequate verification of PIV cre
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of PIV credential verification processes", "2": "Continuous monitori
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2250:
RiskId: 857
ComplianceId: 873
RiskTitle: Risk of unauthorized access and data breaches
Criticality: High
PossibleDamage: Unauthorized access to sensitive information, data breaches, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of sensitive data, financial losses, damage to reputation
RiskDescription: Failure to comply with the requirement of accepting only NIST-compliant external auth

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update the list of accepted external authenticators", "2": "Implement mu
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2251:
RiskId: 858
ComplianceId: 874
RiskTitle: Risk of maintaining an incomplete or inaccurate list of accepted external authenticators
Criticality: Medium
PossibleDamage: Confusion over accepted authenticators, potential security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: Potential unauthorized access, compromised security, operational disruptions
RiskDescription: Failure to maintain an accurate and up-to-date list of accepted external authenticators
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update the list of accepted external authenticators", "2": "Im
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2252:
RiskId: 859

ComplianceId: 875
RiskTitle: Compromised Non-Organizational User Access
Criticality: High
PossibleDamage: Data breaches, unauthorized access to sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Failure to conform to defined identity management profiles may lead to unauthorized a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update and review identity management profiles", "2": "Implement conti
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2253:
RiskId: 345
ComplianceId: 357
RiskTitle: Inaccurate Disclosure of Material Climate-related Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Potential impact on financial performance and stakeholder trust
RiskDescription: Failure to accurately assess and disclose material climate-related risks may lead to fi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear assessment criteria and guidelines", "2": "Engage key stakeholder
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2254:
RiskId: 346
ComplianceId: 358
RiskTitle: Inaccurate Reporting of GHG Emissions
Criticality: High
PossibleDamage: Reputational damage and regulatory fines
Category: Environmental
RiskType: Current
BusinessImpact: Potential financial losses and loss of stakeholder trust
RiskDescription: Failure to accurately report GHG emissions could result in public backlash, legal cons
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data collection and verification processes", "2": "Conduct regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2255:
RiskId: 347
ComplianceId: 359
RiskTitle: Financial Instability due to Climate-related Risks
Criticality: High
PossibleDamage: Significant financial losses and reputational damage

Category: Financial
RiskType: Inherent
BusinessImpact: Disruption to financial planning, budgeting, and strategic decision-making
RiskDescription: Failure to integrate climate risks may result in unanticipated financial losses and dama
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular scenario analysis to identify potential risks", "2": "Diversification of investr
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2256:
RiskId: 348
ComplianceId: 360
RiskTitle: Inaccurate GHG Emissions Reporting
Criticality: High
PossibleDamage: Reputational damage and regulatory fines
Category: Environmental
RiskType: Current
BusinessImpact: Potential financial losses and loss of investor confidence
RiskDescription: Incorrect reporting of GHG emissions could lead to legal and financial repercussions f
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to verify data accuracy", "2": "Training on emission calculation met
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2257:
RiskId: 349
ComplianceId: 361
RiskTitle: Failure to Disclose Material Scope 3 Emissions
Criticality: Medium
PossibleDamage: Investor skepticism and regulatory scrutiny
Category: Environmental
RiskType: Current
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Omission of material Scope 3 emissions could lead to questions about transparency a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement clear materiality thresholds for Scope 3 emissions", "2": "Engage with
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2258:
RiskId: 350
ComplianceId: 362
RiskTitle: Climate Risk Assessment Failure
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, increased climate-related risks
Category: Environmental
RiskType: Inherent
BusinessImpact: Disruption to business operations, financial losses, regulatory scrutiny
RiskDescription: Failure to assess alignment with climate scenarios may lead to increased exposure to

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement climate scenario analysis tools", "2": "Enhance disclosure processes",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2259:
RiskId: 351
ComplianceId: 363
RiskTitle: Failure to Set Climate-Related Targets
Criticality: High
PossibleDamage: Reputational damage, loss of investor confidence, and regulatory fines
Category: Operational
RiskType: Inherent
BusinessImpact: Disruption of sustainability initiatives, decreased stakeholder trust, and financial pena
RiskDescription: Failure to set climate-related targets may result in a lack of direction in managing clim
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on target setting", "2": "Internal audits t
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2260:
RiskId: 352

ComplianceId: 364
RiskTitle: Inaccurate Financial Reporting due to Undisclosed Climate-Related Risks
Criticality: High
PossibleDamage: Financial penalties, loss of investor trust, legal consequences
Category: Operational
RiskType: Inherent
BusinessImpact: Negative impact on financial performance and reputation
RiskDescription: Failure to disclose material climate-related risks can lead to inaccurate financial repor
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear criteria for materiality assessment", "2": "Provide training to financ
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2261:
RiskId: 353
ComplianceId: 365
RiskTitle: Inaccurate Climate-Related Disclosures
Criticality: High
PossibleDamage: Reputational damage, regulatory fines, loss of investor trust
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal implications, reputational harm
RiskDescription: Failure to accurately review climate-related disclosures may result in misleading infor
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement robust review processes", "2": "Regular training on disclosure requiren
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2262:
RiskId: 354
ComplianceId: 366
RiskTitle: Inaccurate Financial Disclosures
Criticality: High
PossibleDamage: Misinformed decision-making, regulatory penalties, and reputational harm
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal repercussions, and damaged reputation
RiskDescription: Misaligned financial disclosures can lead to incorrect assessments of the organizatior
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular alignment checks during financial reporting process", "2": "Training financ
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2263:
RiskId: 355
ComplianceId: 367
RiskTitle: Failure to Identify Regulatory Changes
Criticality: High
PossibleDamage: Non-compliance penalties and fines

Category: Financial
RiskType: Inherent
BusinessImpact: Financial losses and damage to reputation
RiskDescription: Failure to identify regulatory changes could result in non-compliance penalties and fin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly monitor regulatory changes", "2": "Engage legal counsel for compliance
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2264:
RiskId: 356
ComplianceId: 368
RiskTitle: Inaccurate Financial Disclosures
Criticality: High
PossibleDamage: Loss of investor trust, regulatory fines, legal liabilities
Category: Operational
RiskType: Inherent
BusinessImpact: Negative impact on investor confidence, financial performance, and organizational re
RiskDescription: Failure to accurately disclose financial impacts of climate-related risks and opportuniti
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust internal controls for financial reporting", "2": "Conduct regular au
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2265:
RiskId: 357
ComplianceId: 369
RiskTitle: Failure to Conduct Annual Physical Risk Assessment
Criticality: High
PossibleDamage: Increased property damage and operational disruptions
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to conduct annual physical risk assessments may leave the organization vulne
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement risk mitigation measures based on assessment findings", "2": "Regular
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2266:
RiskId: 358
ComplianceId: 370
RiskTitle: Missed Market Opportunities
Criticality: High
PossibleDamage: Loss of competitive advantage and innovation potential
Category: Operational
RiskType: Inherent
BusinessImpact: All business units
RiskDescription: Failure to identify and capitalize on emerging market trends and technologies could re

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear review processes and timelines", "2": "Ensure cross-functional coll
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2267:
RiskId: 359
ComplianceId: 371
RiskTitle: Ineffective Response Monitoring
Criticality: High
PossibleDamage: Financial losses and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial losses and reputational damage
RiskDescription: Failure to effectively monitor responses to climate-related risks may result in missed o
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for staff on monitoring system usage", "2": "Quarterly re
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2268:
RiskId: 360

ComplianceId: 372
RiskTitle: Failure to Disclose Governance Structures
Criticality: High
PossibleDamage: Legal action, shareholder activism, financial losses
Category: Compliance
RiskType: Current
BusinessImpact: Regulatory fines, reputational damage
RiskDescription: Non-disclosure of governance structures related to climate-related risks can lead to le
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular board oversight reviews", "2": "External audit of disclosure processes", "3
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2269:
RiskId: 361
ComplianceId: 373
RiskTitle: Inaccurate Disclosure of Climate-Related Risks
Criticality: High
PossibleDamage: Loss of investor confidence, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Financial planning, strategic decision-making, stakeholder relationships
RiskDescription: Failure to accurately disclose climate-related risks in financial reports may lead to mis
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular risk assessments and scenario analysis", "2": "Engagement with climate
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2270:
RiskId: 362
ComplianceId: 374
RiskTitle: Outdated Climate-Related Risk Assessments
Criticality: Medium
PossibleDamage: Lack of preparedness for climate-related challenges, missed opportunities, strategic
Category: Strategic
RiskType: Residual
BusinessImpact: Strategic planning, competitive positioning, operational resilience
RiskDescription: Failure to update climate-related risk assessments annually may result in strategic mi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on climate risk identification and assessment", "2": "Integration of
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2271:
RiskId: 363
ComplianceId: 375
RiskTitle: Inadequate Disclosure of Risk Management Processes
Criticality: High
PossibleDamage: Loss of investor trust, regulatory fines, reputational damage

Category: Operational
RiskType: Current
BusinessImpact: All business units could be impacted by inadequate risk management processes
RiskDescription: Failure to disclose accurate risk management processes related to climate risks could
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update risk management processes", "2": "Conduct regular reviews of r
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2272:
RiskId: 364
ComplianceId: 376
RiskTitle: Inaccurate Emissions Reporting
Criticality: High
PossibleDamage: Legal fines, reputational damage, loss of investor confidence
Category: Environmental
RiskType: Residual
BusinessImpact: Potential legal liabilities and loss of stakeholder trust
RiskDescription: Failure to accurately report emissions data could result in regulatory fines, reputationa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated emissions tracking systems", "2": "Conduct regular third-pa
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2273:
RiskId: 386
ComplianceId: 398
RiskTitle: Ineffective Establishment of Key Metrics and Targets
Criticality: High
PossibleDamage: Ineffective risk management and missed opportunities for improvement.
Category: Operational
RiskType: Inherent
BusinessImpact: Compromised sustainability and financial performance.
RiskDescription: Failure to establish key metrics and targets may lead to inaccurate risk assessment a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for relevant teams", "2": "Continuous m
CreatedAt: 2025-10-09 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2274:
RiskId: 387
ComplianceId: 399
RiskTitle: Inaccurate GHG Emissions Reporting
Criticality: High
PossibleDamage: Regulatory fines, reputational damage, loss of stakeholder trust
Category: Environmental
RiskType: Current
BusinessImpact: Financial penalties, stakeholder backlash, decreased investor confidence
RiskDescription: Failure to accurately report GHG emissions may result in regulatory investigations, fin

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on GHG Protocol methodology", "2": "Internal audits to ensure ac
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2275:
RiskId: 388
ComplianceId: 400
RiskTitle: Lack of Historical GHG Emissions Data
Criticality: Medium
PossibleDamage: Inaccurate trend analysis, hindered decision-making processes
Category: Environmental
RiskType: Current
BusinessImpact: Inability to track progress towards emission reduction goals, misinformed decision-ma
RiskDescription: Failure to provide historical GHG emissions data may hinder accurate trend analysis,
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish data tracking systems for historical emissions", "2": "Regularly update h
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2276:
RiskId: 389

ComplianceId: 401
RiskTitle: Misalignment of Incentives with Climate Goals
Criticality: High
PossibleDamage: Financial losses, decreased employee morale, reputational harm
Category: Operational
RiskType: Current
BusinessImpact: Impact on financial performance, employee engagement, and organizational reputatio
RiskDescription: Failure to align compensation with climate goals may lead to decreased motivation, fi
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of climate metrics integration", "2": "Employee training on clim
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2277:
RiskId: 390
ComplianceId: 402
RiskTitle: Inaccurate Reporting of Carbon-Related Assets
Criticality: High
PossibleDamage: Misrepresentation of carbon-related assets and lending activities
Category: Operational
RiskType: Residual
BusinessImpact: Financial penalties, reputational damage
RiskDescription: Failure to accurately report carbon-related assets and lending activities may lead to re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement regular audits to verify data accuracy", "2": "Provide training to finance
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2278:
RiskId: 392
ComplianceId: 404
RiskTitle: Outdated Climate-Related Targets
Criticality: Medium
PossibleDamage: Outdated targets may lead to misinformed decision-making, non-compliance penalti
Category: Compliance
RiskType: Current
BusinessImpact: Operational inefficiencies, reputational damage, regulatory fines
RiskDescription: Failure to review and update climate-related targets annually may result in outdated ir
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing clear timeline for annual target reviews", "2": "Regular communicatio
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2279:
RiskId: 393
ComplianceId: 405
RiskTitle: Inaccurate Reporting of Scope 3 GHG Emissions
Criticality: High
PossibleDamage: Misrepresentation of environmental impact, potential fines or penalties

Category: Environmental
RiskType: Current
BusinessImpact: Potential regulatory fines, damage to reputation
RiskDescription: Failure to accurately report Scope 3 GHG emissions may lead to regulatory non-comp
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training on GHG emissions reporting", "2": "Utilize external aud
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2280:
RiskId: 394
ComplianceId: 406
RiskTitle: Inadequate Climate-Related Updates to Board
Criticality: High
PossibleDamage: Uninformed decision-making, regulatory non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Impaired decision-making, reputational damage
RiskDescription: Failure to provide timely and accurate climate-related updates to the board may result
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting guidelines and timelines for the risk management commi
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2281:
RiskId: 395
ComplianceId: 407
RiskTitle: Lack of Assigned Climate-Related Responsibilities
Criticality: High
PossibleDamage: Ineffective climate risk management and missed opportunities for improvement
Category: Environmental
RiskType: Inherent
BusinessImpact: Reduced ability to proactively address climate risks and capitalize on opportunities
RiskDescription: Failure to assign responsibilities may lead to confusion, lack of focus, and missed opp
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on climate-related responsibilities", "2": "Performance e
CreatedAt: 2025-10-09 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2282:
RiskId: 400
ComplianceId: 412
RiskTitle: Non-disclosure of GHG emissions
Criticality: High
PossibleDamage: Legal fines, reputational damage, loss of investor trust
Category: Environmental
RiskType: Current
BusinessImpact: Financial losses, decreased market value
RiskDescription: Failure to disclose GHG emissions can result in legal and financial repercussions, as

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust reporting processes", "2": "Engage with stakeholders to addres
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2283:
RiskId: 401
ComplianceId: 413
RiskTitle: Inaccurate Assessment of Climate-Related Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Operational
RiskType: Current
BusinessImpact: May lead to misinformed decision-making, increased operational costs, and loss of in
RiskDescription: Failure to accurately assess climate-related risks may result in inadequate mitigation s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and review of metrics and targets", "2": "Engagement with ind
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2284:
RiskId: 402

ComplianceId: 414
RiskTitle: Governance Disclosure Non-Compliance Risk
Criticality: High
PossibleDamage: Loss of stakeholder trust, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to comply with governance disclosure requirements could result in regulatory p
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular internal audits to assess governance framework", "2": "Timely updates in
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2285:
RiskId: 403
ComplianceId: 415
RiskTitle: Lack of Clear Accountability for Climate-Related Issues
Criticality: High
PossibleDamage: Ineffective management of climate-related risks and missed opportunities
Category: Environmental
RiskType: Inherent
BusinessImpact: Potential reputational damage and financial losses
RiskDescription: Failure to assign clear responsibilities may result in confusion, lack of oversight, and r
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear job descriptions and responsibilities for designated positions", "2":
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2286:
RiskId: 404
ComplianceId: 416
RiskTitle: Lack of Regular Reporting to the Board
Criticality: Medium
PossibleDamage: Inadequate oversight of climate-related risks and missed opportunities
Category: Operational
RiskType: Inherent
BusinessImpact: Challenges in decision-making and risk management for designated roles
RiskDescription: Failure to report regularly may result in uninformed decision-making by the board, lea
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting timelines and formats for designated roles", "2": "Provide
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2287:
RiskId: 405
ComplianceId: 417
RiskTitle: Failure to Conduct Annual Review of Climate-Related Risks
Criticality: High
PossibleDamage: Uninformed investment decisions and operational planning

Category: Operational
RiskType: Current
BusinessImpact: All business units may be impacted by uninformed decision-making
RiskDescription: Failure to conduct the annual review may result in the organization missing out on key
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Engage external climate experts for insights", "2": "Regular training for staff on cli
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2288:
RiskId: 406
ComplianceId: 418
RiskTitle: Lack of Cross-Departmental Collaboration for Climate Risk Review
Criticality: Medium
PossibleDamage: Overlooking critical climate-related risks and opportunities
Category: Operational
RiskType: Current
BusinessImpact: Strategic planning, finance, operations, sustainability teams may be impacted by lack
RiskDescription: Failure to involve cross-departmental collaboration in the climate risk review process
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels between departments", "2": "Hold regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2289:
RiskId: 407
ComplianceId: 419
RiskTitle: Inaccurate Reporting and Missed Targets
Criticality: High
PossibleDamage: Inaccurate reporting may lead to misinformed decision-making, missed targets, and
Category: Operational
RiskType: Current
BusinessImpact: All business units within the organization may be impacted by inaccurate reporting an
RiskDescription: Failure to accurately monitor and report progress against climate-related goals may re
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on data collection and reporting proces
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2290:
RiskId: 408
ComplianceId: 420
RiskTitle: Unidentified Climate-related Risks
Criticality: High
PossibleDamage: Financial losses and reputational damage
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to identify and address climate-related risks could lead to financial instability a

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement risk management strategies based on assessment results", "2": "Deve
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2291:
RiskId: 409
ComplianceId: 421
RiskTitle: Inaccurate Financial Planning due to Climate Factors
Criticality: High
PossibleDamage: Budget shortfalls, increased costs, missed revenue opportunities
Category: Financial
RiskType: Residual
BusinessImpact: Negative impact on financial performance and strategic goals
RiskDescription: Failure to integrate climate issues into financial planning may result in inaccurate bud
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for finance team on climate-related financial impacts", "2": "Estab
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2292:
RiskId: 410

ComplianceId: 422
RiskTitle: Inadequate Climate Risk Preparedness
Criticality: High
PossibleDamage: Financial losses, strategic misalignment
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses and strategic misalignment
RiskDescription: Failure to comply with biennial scenario analysis may result in inadequate preparedne
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs on climate-related risks", "2": "Engage
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2293:
RiskId: 411
ComplianceId: 423
RiskTitle: Failure to Identify and Assess Climate-Related Risks
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory penalties
Category: Environmental
RiskType: Current
BusinessImpact: Potential disruption of operations, increased costs for risk mitigation
RiskDescription: Inadequate identification and assessment of climate-related risks may lead to unantic
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training on risk identification and assessment processes", "2": "Engagem
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2294:
RiskId: 412
ComplianceId: 424
RiskTitle: Failure to Manage Climate-Related Risks Effectively
Criticality: High
PossibleDamage: Financial losses, reputational damage, regulatory fines
Category: Environmental
RiskType: Inherent
BusinessImpact: Potential disruption to operations, increased costs, loss of stakeholder trust
RiskDescription: Inadequate management of climate-related risks may lead to business interruptions a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establishing clear risk management processes", "2": "Regular risk assessments",
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2295:
RiskId: 413
ComplianceId: 425
RiskTitle: Inadequate Documentation of Climate-Related Risk Integration
Criticality: High
PossibleDamage: Increased exposure to climate-related risks and potential financial losses

Category: Operational
RiskType: Inherent
BusinessImpact: Potential disruption to operations and financial performance
RiskDescription: Failure to document integration may lead to ineffective risk management strategies ar
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on documentation requirements", "2": "Establish clear documenta
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2296:
RiskId: 414
ComplianceId: 426
RiskTitle: Misreporting of GHG Emissions
Criticality: High
PossibleDamage: Reputational damage, regulatory fines
Category: Environmental
RiskType: Current
BusinessImpact: Loss of investor confidence, legal implications
RiskDescription: Incorrect reporting of GHG emissions leading to inaccurate environmental performanc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust GHG emission tracking systems", "2": "Regularly audit emissior
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2297:
RiskId: 415
ComplianceId: 427
RiskTitle: Non-Alignment with Reporting Frameworks
Criticality: Medium
PossibleDamage: Inaccurate reporting, lack of transparency
Category: Operational
RiskType: Current
BusinessImpact: Loss of stakeholder trust, misinformed decision-making
RiskDescription: Failure to adhere to established reporting frameworks leading to inconsistent and unre
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Training on reporting frameworks for relevant staff", "2": "Regular audits to ensure
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2298:
RiskId: 416
ComplianceId: 428
RiskTitle: Inaccurate Forward-Looking Metrics Disclosure
Criticality: High
PossibleDamage: Loss of stakeholder trust, regulatory fines, reputational damage
Category: Environmental
RiskType: Inherent
BusinessImpact: Negative impact on sustainability reporting credibility and stakeholder relationships
RiskDescription: Failure to provide accurate forward-looking metrics and targets in sustainability report

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting of metrics", "2": "Engagement with stakeholders
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2299:
RiskId: 417
ComplianceId: 429
RiskTitle: Inaccurate Reporting of Climate Metrics
Criticality: High
PossibleDamage: Loss of stakeholder trust, regulatory fines, reputational damage
Category: Compliance
RiskType: Inherent
BusinessImpact: Impact on stakeholder trust, regulatory compliance, and investor confidence
RiskDescription: Failure to accurately report climate-related metrics can lead to legal and financial cons
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and updates on climate metrics calculation methodologies", "2": "
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2300:
RiskId: 418

ComplianceId: 430
RiskTitle: Outdated Methodologies for Climate Metrics Calculation
Criticality: Medium
PossibleDamage: Inaccurate reporting and misrepresentation of climate impact
Category: Compliance
RiskType: Inherent
BusinessImpact: Loss of stakeholder trust, regulatory non-compliance, and reputational damage
RiskDescription: Failure to update methodologies annually can result in inaccurate reporting of climate
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a regular review schedule for methodologies", "2": "Engage external cor
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2301:
RiskId: 419
ComplianceId: 431
RiskTitle: Inaccurate Reporting of Scope 3 GHG Emissions
Criticality: High
PossibleDamage: Financial penalties, reputational damage, loss of stakeholder trust
Category: Environmental
RiskType: Current
BusinessImpact: Potential impact on financial disclosures and organizational reputation
RiskDescription: Failure to accurately report Scope 3 GHG emissions may result in regulatory fines, re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular training on GHG Protocol methodology", "2": "Internal audits to verify dat
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2302:
RiskId: 420
ComplianceId: 432
RiskTitle: Misrepresentation of Climate-Related Performance
Criticality: High
PossibleDamage: Damage to reputation and credibility, potential legal implications.
Category: Environmental
RiskType: Inherent
BusinessImpact: Loss of stakeholder trust, negative impact on investment decisions.
RiskDescription: Failure to disclose relevant carbon footprinting metrics may lead to misrepresentation
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions for sustainability and reporting teams on identifying and
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2303:
RiskId: 421
ComplianceId: 433
RiskTitle: Non-alignment of Climate-Related Targets
Criticality: High
PossibleDamage: Missed environmental goals, regulatory non-compliance, reputational damage

Category: Environmental
RiskType: Current
BusinessImpact: Negative impact on sustainability initiatives, regulatory standing, and stakeholder rela
RiskDescription: Failure to align climate-related targets with organizational goals may lead to missed e
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring and reporting of progress towards targets", "2": "Engage stake
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2304:
RiskId: 422
ComplianceId: 434
RiskTitle: Misreporting of Climate-Related Data
Criticality: High
PossibleDamage: Loss of investor trust, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Finance, Sustainability
RiskDescription: Inaccurate reporting of progress against climate-related targets leading to regulatory r
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust data collection and verification processes", "2": "Conduct regula
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2305:
RiskId: 423
ComplianceId: 435
RiskTitle: Missed Quarterly Board Meetings on Climate-related Risks
Criticality: High
PossibleDamage: Inadequate oversight of climate-related risks and missed strategic opportunities
Category: Operational
RiskType: Current
BusinessImpact: Board decision-making and strategic planning may be compromised.
RiskDescription: Failure to meet quarterly meetings may result in inadequate oversight of climate-relate
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Schedule make-up meetings if quarterly meetings are missed", "2": "Provide boar
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2306:
RiskId: 424
ComplianceId: 436
RiskTitle: Exclusion of Climate Considerations in Budgets and Strategic Plans
Criticality: Medium
PossibleDamage: Missed opportunities for sustainable growth and resilience
Category: Financial
RiskType: Current
BusinessImpact: Financial performance and strategic direction may be compromised.
RiskDescription: Failure to integrate climate considerations may result in missed opportunities for susta

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a dedicated climate budget line item", "2": "Include climate impact asses
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2307:
RiskId: 425
ComplianceId: 437
RiskTitle: Lack of Designated Management Positions for Climate Risk Management
Criticality: High
PossibleDamage: Failure to designate management-level positions may result in lack of oversight and
Category: Operational
RiskType: Inherent
BusinessImpact: All business units would be impacted by ineffective management of climate risks.
RiskDescription: The lack of designated management positions may lead to confusion, lack of account
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and awareness programs for designated positions", "2": "Establis
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2308:
RiskId: 426

ComplianceId: 438
RiskTitle: Failure to Integrate Climate Risks into Operational Planning
Criticality: Medium
PossibleDamage: Failure to integrate climate risks into operational planning may result in uninformed d
Category: Operational
RiskType: Inherent
BusinessImpact: All business units would be impacted by ineffective integration of climate risks into op
RiskDescription: The failure to incorporate climate risks into operational planning and decision-making
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular risk assessments and scenario planning exercises", "2": "Establish clear
CreatedAt: 2025-10-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2309:
RiskId: 1
ComplianceId: 1
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Unauthorized access to cardholder data leading to data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement encryption for sensitive data", "2": "Regularly monitor access logs", "3"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2310:
RiskId: 2
ComplianceId: 2
RiskTitle: Vulnerability Post-Change Risk
Criticality: Medium
PossibleDamage: Data breaches, system downtime
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Unaddressed vulnerabilities post-change leading to potential data breaches
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated vulnerability scanning post-change", "2": "Conduct regular s
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2311:
RiskId: 3
ComplianceId: 3
RiskTitle: Cloud Data Breach Risk
Criticality: High
PossibleDamage: Data breaches, regulatory fines

Category: IT
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Data breaches in cloud environments leading to potential loss of cardholder data
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement cloud access controls", "2": "Regularly monitor cloud activity", "3": "Imp
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2312:
RiskId: 4
ComplianceId: 4
RiskTitle: Failure to Remediate Identified Vulnerabilities
Criticality: High
PossibleDamage: Unauthorized access to cardholder data, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties
RiskDescription: Failure to remediate identified vulnerabilities within the specified timeframe may result
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated vulnerability scanning tools", "2": "Establish a remediation t
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2313:
RiskId: 5
ComplianceId: 5
RiskTitle: Failure to Implement Secure Configurations
Criticality: Medium
PossibleDamage: Data breaches, non-compliance with industry standards
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Failure to implement secure configurations on systems handling cardholder data may
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Use configuration management tools to enforce secure settings", "2": "Regularly a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2314:
RiskId: 6
ComplianceId: 6
RiskTitle: Failure to Implement Patch Management Process
Criticality: High
PossibleDamage: System compromise, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Failure to implement a patch management process may leave systems vulnerable to

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a patch management process with defined timelines", "2": "Test patches
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2315:
RiskId: 7
ComplianceId: 7
RiskTitle: Failure to Submit Quarterly Compliance Report
Criticality: High
PossibleDamage: Fines, penalties, loss of business opportunities
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, reputational damage
RiskDescription: Failure to submit quarterly compliance reports may lead to regulatory scrutiny, fines, a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting deadlines and responsibilities", "2": "Implement regular r
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2316:
RiskId: 8

ComplianceId: 8
RiskTitle: Incomplete Documentation of Remediation Actions
Criticality: Medium
PossibleDamage: Recurring compliance issues, financial penalties
Category: Operational
RiskType: Current
BusinessImpact: Regulatory penalties, reputational damage
RiskDescription: Lack of documentation for remediation actions may lead to incomplete compliance eff
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear documentation guidelines and templates", "2": "Assign responsibil
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2317:
RiskId: 9
ComplianceId: 9
RiskTitle: Failure to Report Completion of Remediation Actions
Criticality: High
PossibleDamage: Loss of stakeholder trust, business opportunities
Category: Operational
RiskType: Current
BusinessImpact: Reputational damage, loss of business opportunities
RiskDescription: Failure to report completion of remediation actions may lead to stakeholders being un
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear reporting deadlines and responsibilities", "2": "Implement regular r
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2318:
RiskId: 10
ComplianceId: 10
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties
RiskDescription: Unauthorized access to cardholder data can lead to data breaches and financial losse
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular access reviews to ensure access controls are up to date", "2": "Implemen
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2319:
RiskId: 11
ComplianceId: 11
RiskTitle: Outdated Access Controls
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches

Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, regulatory non-compliance
RiskDescription: Outdated access controls can lead to unauthorized access and data breaches, resulti
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate access review processes to ensure timely reviews", "2": "Implement reg
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2320:
RiskId: 12
ComplianceId: 12
RiskTitle: Undetected Unauthorized Access
Criticality: High
PossibleDamage: Data breaches, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Legal penalties, loss of customer trust
RiskDescription: Undetected unauthorized access can lead to data breaches and legal consequences,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement real-time monitoring of access logs", "2": "Regularly analyze access lo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2321:
RiskId: 13
ComplianceId: 13
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal implications, loss of customer trust
RiskDescription: Risk of unauthorized access to cardholder data during transmission over public netwo
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption protocols", "2": "Regularly update encryption standar
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2322:
RiskId: 14
ComplianceId: 14
RiskTitle: Unauthorized Access to Stored Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal implications, loss of customer trust
RiskDescription: Risk of unauthorized access to cardholder data when stored

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption protocols for data at rest", "2": "Regularly review acc
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2323:
RiskId: 15
ComplianceId: 15
RiskTitle: Non-Compliance with Encryption Protocol Standards
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial losses, legal implications, loss of customer trust
RiskDescription: Risk of using weak encryption protocols for cardholder data protection
RiskLikelihood: 8
RiskImpact: 10
RiskExposureRating: 80
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption protocols to meet industry standards", "2": "Conduct
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2324:
RiskId: 16

ComplianceId: 16
RiskTitle: Outdated Anti-Virus Software
Criticality: High
PossibleDamage: Increased risk of malware infections and data breaches
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, loss of sensitive data, reputational damage
RiskDescription: Failure to update anti-virus software daily can leave systems vulnerable to known thre
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated update mechanisms for anti-virus software", "2": "Regularly
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2325:
RiskId: 17
ComplianceId: 17
RiskTitle: Unidentified Vulnerabilities
Criticality: High
PossibleDamage: Data breaches, system compromise
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, reputational damage, financial losses
RiskDescription: Failure to conduct monthly vulnerability scans can leave systems exposed to known v
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Utilize automated vulnerability scanning tools", "2": "Establish a process for timely
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2326:
RiskId: 18
ComplianceId: 18
RiskTitle: Delayed Security Patch Application
Criticality: High
PossibleDamage: Increased risk of security incidents
Category: IT
RiskType: Residual
BusinessImpact: Data breaches, system compromise, financial losses
RiskDescription: Failure to apply security patches promptly can leave systems vulnerable to known vul
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 75.44
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a patch management process", "2": "Regularly monitor security advisori
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2327:
RiskId: 19
ComplianceId: 19
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Failure to document firewall and router configurations may lead to unauthorized acces
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of configuration documentation", "2": "Training on proper documen
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2328:
RiskId: 20
ComplianceId: 20
RiskTitle: Security Vulnerabilities Due to Inadequate Testing
Criticality: Medium
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Disruption of services, financial losses
RiskDescription: Failure to conduct formal testing of firewall and router configurations may leave syste
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated testing tools", "2": "Regular security audits", "3": "Continuous monitori
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2329:
RiskId: 21
ComplianceId: 21
RiskTitle: Security Vulnerabilities Due to Outdated Configurations
Criticality: High
PossibleDamage: Data breaches, unauthorized access
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, regulatory fines
RiskDescription: Failure to review firewall and router configurations regularly may expose systems to s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular configuration reviews", "2": "Automated alerts for configuration changes",
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2330:
RiskId: 22
ComplianceId: 22
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Unauthorized access to cardholder data due to inadequate firewall restrictions from u

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update firewall rules to adapt to new threats", "2": "Implement intrusion
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2331:
RiskId: 23
ComplianceId: 23
RiskTitle: Outdated Firewall Configurations
Criticality: Medium
PossibleDamage: Vulnerabilities, potential data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory fines
RiskDescription: Outdated firewall configurations due to lack of regular reviews and updates, leading to
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Document and track changes made during each review", "2": "Conduct penetratio
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2332:
RiskId: 24

ComplianceId: 24
RiskTitle: Unauthorized Access and Malware Infections
Criticality: High
PossibleDamage: Data breaches, malware infections
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, system downtime
RiskDescription: Unauthorized access to cardholder data and potential malware infections due to inade
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly monitor network traffic for anomalies", "2": "Implement network segmen
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2333:
RiskId: 25
ComplianceId: 25
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: IT
RiskType: Residual
BusinessImpact: Data loss, regulatory fines
RiskDescription: Unauthorized access to cardholder data can lead to data breaches and financial losse
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement firewall rules to restrict access", "2": "Regularly monitor network traffic
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2334:
RiskId: 26
ComplianceId: 26
RiskTitle: Access Control Risk
Criticality: Medium
PossibleDamage: Data breaches, compliance violations
Category: IT
RiskType: Residual
BusinessImpact: Data exposure, regulatory fines
RiskDescription: Inadequate access controls can lead to unauthorized access to cardholder data and c
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement role-based access control", "2": "Regularly review access permissions"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2335:
RiskId: 27
ComplianceId: 27
RiskTitle: Continuous Monitoring Risk
Criticality: High
PossibleDamage: Data breaches, financial losses

Category: IT
RiskType: Residual
BusinessImpact: Data exposure, financial liabilities
RiskDescription: Lack of continuous monitoring can lead to undetected unauthorized access attempts a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement intrusion detection systems", "2": "Regularly conduct security audits", "
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2336:
RiskId: 28
ComplianceId: 28
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal liabilities, loss of customer trust
RiskDescription: Unauthorized access to cardholder data through devices without firewall protection
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update firewall software", "2": "Monitor firewall configurations for compli
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2337:
RiskId: 29
ComplianceId: 29
RiskTitle: Incompatibility Issues with Firewall Software
Criticality: Medium
PossibleDamage: Security vulnerabilities, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Disruption of services, data breaches
RiskDescription: Usage of unapproved firewall software leading to compatibility issues and security vul
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update approved firewall software", "2": "Implement strict software appr
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2338:
RiskId: 30
ComplianceId: 30
RiskTitle: Misconfigured Firewall Settings
Criticality: High
PossibleDamage: Security gaps, unauthorized access
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, compliance violations
RiskDescription: Misconfigured firewall settings leading to security vulnerabilities and unauthorized acc

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated configuration checks", "2": "Conduct manual configuration a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2339:
RiskId: 31
ComplianceId: 31
RiskTitle: Outdated Security Policies
Criticality: High
PossibleDamage: Increased risk of security breaches and data loss
Category: Operational
RiskType: Residual
BusinessImpact: IT Security, Compliance
RiskDescription: Failure to update security policies annually may expose the organization to cyber thre
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Employee training on policy changes",
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2340:
RiskId: 32

ComplianceId: 32
RiskTitle: Lack of Centralized Documentation Repository
Criticality: Medium
PossibleDamage: Increased risk of non-compliance, misconfigurations, and security incidents
Category: Operational
RiskType: Residual
BusinessImpact: IT Security, Compliance, Operations
RiskDescription: Without a centralized repository, personnel may struggle to find and adhere to securit
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement access controls to the repository", "2": "Regularly update and organize
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2341:
RiskId: 33
ComplianceId: 33
RiskTitle: Lack of Compliance Officer Oversight
Criticality: High
PossibleDamage: Increased risk of non-compliance, regulatory fines, and reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Compliance
RiskDescription: Without proper oversight, security policies may not be accurately documented, leadin
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular reviews of policy documentation", "2": "Training on policy documentation
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2342:
RiskId: 34
ComplianceId: 34
RiskTitle: Unauthorized Access Due to Default Passwords
Criticality: High
PossibleDamage: Potential data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Data security, reputation
RiskDescription: Unauthorized users gaining access to sensitive data due to default passwords
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Regularly audit password changes", "3
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2343:
RiskId: 35
ComplianceId: 35
RiskTitle: Unauthorized Access Post-Deployment
Criticality: High
PossibleDamage: Potential data breaches, loss of sensitive information

Category: IT
RiskType: Residual
BusinessImpact: Data security, reputation
RiskDescription: Unauthorized users gaining access to sensitive data post-deployment due to default p
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 65.1
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Regularly audit password changes", "3
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2344:
RiskId: 36
ComplianceId: 36
RiskTitle: Unauthorized Access Due to Default Accounts
Criticality: Medium
PossibleDamage: Potential data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Data security, reputation
RiskDescription: Attackers exploiting unnecessary default accounts to gain unauthorized access
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 48.75
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and disable unused accounts", "2": "Implement access controls"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2345:
RiskId: 37
ComplianceId: 37
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: IT
RiskType: Residual
BusinessImpact: IT infrastructure and data security
RiskDescription: Unauthorized access to sensitive data due to lack of proper configuration standards
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular security training for IT team members", "2": "Implementing multi-factor au
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2346:
RiskId: 38
ComplianceId: 38
RiskTitle: Outdated Configuration Standards Risk
Criticality: Medium
PossibleDamage: Exploitation of outdated vulnerabilities, data breaches
Category: IT
RiskType: Residual
BusinessImpact: IT infrastructure and data security
RiskDescription: Exploitation of vulnerabilities due to outdated configuration standards

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular vulnerability assessments", "2": "Continuous monitoring of system compo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2347:
RiskId: 39
ComplianceId: 39
RiskTitle: Non-alignment with Industry Best Practices Risk
Criticality: High
PossibleDamage: Security breaches, data leaks, reputation damage
Category: IT
RiskType: Residual
BusinessImpact: IT infrastructure and data security
RiskDescription: Security vulnerabilities due to non-alignment with industry best practices
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular industry benchmarking", "2": "Engagement with industry experts", "3": "P
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2348:
RiskId: 40

ComplianceId: 40
RiskTitle: Data Breach due to Unencrypted Administrative Access
Criticality: High
PossibleDamage: Loss of sensitive data, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Disruption of business operations, financial losses
RiskDescription: Unauthorized individuals gaining access to sensitive data through unencrypted admin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption algorithms", "2": "Regular security audits and assess
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2349:
RiskId: 41
ComplianceId: 41
RiskTitle: Security Vulnerabilities due to Outdated Encryption Methods
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory fines
RiskDescription: Failure to update encryption methods may expose systems to known vulnerabilities a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regular encryption method updates", "2": "Automated vulnerability scanning", "3"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2350:
RiskId: 42
ComplianceId: 42
RiskTitle: Security Breach from Unauthorized Encryption Methods
Criticality: Medium
PossibleDamage: Data loss, system compromise
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Use of unapproved encryption methods may lead to vulnerabilities that can be exploit
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Enforce encryption policy through access controls", "2": "Regular validation of enc
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2351:
RiskId: 43
ComplianceId: 43
RiskTitle: Unauthorized Access to Payment Card Data
Criticality: High
PossibleDamage: Loss of customer trust, financial penalties

Category: Operational
RiskType: Residual
BusinessImpact: Disruption of payment processing, financial loss
RiskDescription: Unauthorized access to payment card data due to outdated or missing components in
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication for system access", "2": "Encrypt sensitive d
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2352:
RiskId: 44
ComplianceId: 44
RiskTitle: Unidentified Vulnerabilities in the System
Criticality: Medium
PossibleDamage: Data breaches, system downtime
Category: IT
RiskType: Residual
BusinessImpact: Data loss, financial loss
RiskDescription: Unidentified vulnerabilities in the system due to inaccurate tracking of components.
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular vulnerability scans and assessments", "2": "Implement patch manageme
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2353:
RiskId: 45
ComplianceId: 45
RiskTitle: Non-Compliance with PCI DSS Requirements
Criticality: Low
PossibleDamage: Fines, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Financial penalties, loss of customer trust
RiskDescription: Non-compliance with PCI DSS requirements due to exclusion of systems involved in p
RiskLikelihood: 3
RiskImpact: 5
RiskExposureRating: 15
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Regular PCI DSS compliance assessments", "2": "Implement continuous monitori
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2354:
RiskId: 46
ComplianceId: 46
RiskTitle: Outdated Security Policies
Criticality: High
PossibleDamage: Security breaches and data loss
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, reputation damage
RiskDescription: Failure to review security policies annually could result in outdated procedures that ar

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Continuous monitoring of policy effecti
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2355:
RiskId: 47
ComplianceId: 47
RiskTitle: Unauthorized Access to Policies
Criticality: Medium
PossibleDamage: Security breaches and data exposure
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, legal consequences
RiskDescription: Failure to maintain a centralized repository accessible to all personnel could result in
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Access control mechanisms on repository", "2": "Regular access reviews and per
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2356:
RiskId: 48

ComplianceId: 48
RiskTitle: Undefined Operational Procedures
Criticality: High
PossibleDamage: Password management errors and security incidents
Category: Operational
RiskType: Residual
BusinessImpact: Data loss, system downtime
RiskDescription: Failure to document operational procedures related to password management could r
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular procedure documentation updates", "2": "Employee training on procedure
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2357:
RiskId: 49
ComplianceId: 49
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Potential data breaches and regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial losses
RiskDescription: Unauthorized access to stored cardholder data can lead to data breaches and regulat
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement access controls and encryption for stored data", "2": "Regularly monito
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2358:
RiskId: 50
ComplianceId: 50
RiskTitle: Outdated Data Storage Policies
Criticality: Medium
PossibleDamage: Non-compliance with data storage regulations
Category: Operational
RiskType: Residual
BusinessImpact: Regulatory fines, reputational damage
RiskDescription: Outdated data storage policies may lead to non-compliance with regulations and pote
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update data policies", "2": "Conduct internal audits to ensure
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2359:
RiskId: 51
ComplianceId: 51
RiskTitle: Accumulation of Unnecessary Data
Criticality: High
PossibleDamage: Increased risk of data breaches

Category: Operational
RiskType: Residual
BusinessImpact: Data security vulnerabilities, regulatory fines
RiskDescription: Accumulation of unnecessary data increases the risk of data breaches and non-comp
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated data purging processes", "2": "Regularly review data storag
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2360:
RiskId: 52
ComplianceId: 52
RiskTitle: Unauthorized Access to Sensitive Authentication Data
Criticality: High
PossibleDamage: Financial loss, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches leading to financial loss and reputational damage
RiskDescription: Unauthorized access to stored sensitive authentication data can lead to data breache
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement tokenization or encryption of sensitive data", "2": "Regularly audit syste
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2361:
RiskId: 53
ComplianceId: 53
RiskTitle: Non-Compliance with Data Handling Procedures
Criticality: Medium
PossibleDamage: Data breaches
Category: Operational
RiskType: Current
BusinessImpact: Failure to identify non-compliance leading to data breaches
RiskDescription: Non-compliance with data handling procedures can result in unauthorized data storag
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated auditing tools", "2": "Provide regular training on data handli
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2362:
RiskId: 54
ComplianceId: 54
RiskTitle: Employee Error in Data Handling
Criticality: Low
PossibleDamage: Data breaches
Category: Operational
RiskType: Current
BusinessImpact: Employee error leading to non-compliance and potential data breaches
RiskDescription: Employee error in data handling can result in unauthorized data storage and potential

RiskLikelihood: 5
RiskImpact: 4
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Develop comprehensive training materials", "2": "Conduct regular training session
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2363:
RiskId: 55
ComplianceId: 55
RiskTitle: Unauthorized Access to PAN Data
Criticality: High
PossibleDamage: Exposure of sensitive cardholder data leading to potential fraud
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Unauthorized access to PAN data can lead to fraudulent activities and financial losses
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for stored PAN data", "2": "Regularly monitor access to PAN
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2364:
RiskId: 56

ComplianceId: 56
RiskTitle: Exposure of PAN in Log Files
Criticality: Medium
PossibleDamage: Exposure of sensitive cardholder data in log files
Category: IT
RiskType: Residual
BusinessImpact: Compromised security, regulatory fines
RiskDescription: Exposure of PAN in log files can lead to compromised security and regulatory non-co
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement log file encryption", "2": "Regularly review and rotate log files", "3": "Im
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2365:
RiskId: 57
ComplianceId: 57
RiskTitle: Exposure of PAN in Database Queries
Criticality: High
PossibleDamage: Exposure of sensitive cardholder data in database queries
Category: IT
RiskType: Residual
BusinessImpact: Data breaches, regulatory fines
RiskDescription: Exposure of PAN in database queries can lead to data breaches and regulatory non-c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement parameterized queries", "2": "Use stored procedures for PAN retrieval'
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2366:
RiskId: 58
ComplianceId: 58
RiskTitle: Data Breach due to Unencrypted PAN Data
Criticality: High
PossibleDamage: Financial loss, reputational damage, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal repercussions
RiskDescription: Unauthorized access to unencrypted PAN data leading to data breach
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption protocols such as AES-256", "2": "Regularly update encryp
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2367:
RiskId: 59
ComplianceId: 59
RiskTitle: Data Breach due to Weak Hashing of PAN Data
Criticality: Medium
PossibleDamage: Financial loss, reputational damage, regulatory fines

Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal repercussions
RiskDescription: Weak hashing algorithms used for PAN data leading to data breach
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement secure hashing algorithms like SHA-256", "2": "Regularly update hash
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2368:
RiskId: 60
ComplianceId: 60
RiskTitle: Data Breach due to Unauthorized Access to PAN Data
Criticality: High
PossibleDamage: Financial loss, reputational damage, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal repercussions
RiskDescription: Unauthorized access to PAN data by unauthorized personnel leading to data breach
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access controls", "2": "Regularly review access permission
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2369:
RiskId: 61
ComplianceId: 61
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of customer trust, financial penalties
Category: Operational
RiskType: Current
BusinessImpact: Loss of revenue, legal consequences
RiskDescription: Unauthorized access to cardholder data leading to potential misuse
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for data at rest and in transit", "2": "Regular security assess
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2370:
RiskId: 62
ComplianceId: 62
RiskTitle: Confusion Risk
Criticality: Medium
PossibleDamage: Non-compliance with policies, errors in data handling
Category: Operational
RiskType: Current
BusinessImpact: Operational inefficiencies, potential data breaches
RiskDescription: Lack of centralized repository leading to outdated or conflicting policies

RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on repository usage", "2": "Implement version control for policies'
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2371:
RiskId: 63
ComplianceId: 63
RiskTitle: Access Restriction Risk
Criticality: Medium
PossibleDamage: Non-compliance with policies, errors in data handling
Category: Operational
RiskType: Current
BusinessImpact: Operational inefficiencies, potential data breaches
RiskDescription: Restricted access leading to personnel not following updated policies
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular access training sessions", "2": "Implement automated policy access remi
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2372:
RiskId: 64

ComplianceId: 64
RiskTitle: Data Breach Due to Weak Encryption
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal consequences.
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines, legal liabilities.
RiskDescription: Failure to implement strong encryption could lead to unauthorized access to cardhold
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption libraries and tools", "2": "Implement multi-factor auth
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2373:
RiskId: 65
ComplianceId: 65
RiskTitle: Non-Compliance with Encryption Standards
Criticality: Medium
PossibleDamage: Penalties, loss of customer trust, data breaches.
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, reputational damage, legal consequences.
RiskDescription: Failure to monitor encryption protocols and conduct compliance audits could result in
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement automated monitoring tools for encryption protocols", "2": "Conduct reg

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: IT Operations Unit

Item 2374:

RiskId: 66

ComplianceId: 66

RiskTitle: Compromised Encryption Keys

Criticality: High

PossibleDamage: Unauthorized access to sensitive data, data breaches.

Category: IT

RiskType: Residual

BusinessImpact: Financial losses, reputational damage, legal consequences.

RiskDescription: Failure to implement secure key management practices and regular key rotation could

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement secure key management practices", "2": "Regularly rotate encryption k

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 2375:

RiskId: 67

ComplianceId: 67

RiskTitle: Compromise of Encryption Keys

Criticality: High

PossibleDamage: Unauthorized access to sensitive data

Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, reputational damage
RiskDescription: Unauthorized access to encryption keys can lead to data breaches and compromise c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular key rotation and updates", "2": "Implement strong access controls for key
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2376:
RiskId: 68
ComplianceId: 68
RiskTitle: Failure to Rotate Encryption Keys
Criticality: Medium
PossibleDamage: Prolonged exposure of sensitive data
Category: IT
RiskType: Residual
BusinessImpact: Increased risk of data breaches
RiskDescription: Failure to rotate encryption keys can lead to prolonged exposure of sensitive data, inc
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate key rotation processes", "2": "Implement key rotation reminders and ale
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2377:
RiskId: 69
ComplianceId: 69
RiskTitle: Unauthorized Access to Stored Keys
Criticality: High
PossibleDamage: Data breaches
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data
RiskDescription: Unauthorized access to stored keys can lead to data breaches and compromise of se
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Use hardware security modules for key storage", "2": "Implement access controls
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2378:
RiskId: 70
ComplianceId: 70
RiskTitle: Outdated Encryption and Key Management Policies
Criticality: High
PossibleDamage: Data breaches and loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: All departments handling cardholder data
RiskDescription: Failure to update encryption and key management policies can lead to vulnerabilities

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on encryption and key management best practices", "2": "Automa
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2379:
RiskId: 71
ComplianceId: 71
RiskTitle: Inconsistent Policy Access and Implementation
Criticality: Medium
PossibleDamage: Inconsistent policy implementation leading to security vulnerabilities
Category: IT
RiskType: Residual
BusinessImpact: All departments handling cardholder data
RiskDescription: Lack of centralized policy management can result in unauthorized changes and incon
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular system maintenance and updates", "2": "Access controls to restrict unaut
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2380:
RiskId: 72

ComplianceId: 72
RiskTitle: Lack of Clarity in Policy Documentation
Criticality: High
PossibleDamage: Miscommunication and misinterpretation of policies
Category: IT
RiskType: Residual
BusinessImpact: All departments handling cardholder data
RiskDescription: Failure to clearly document and communicate policies can lead to misunderstandings
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for Compliance Officer on policy documentation best practices", "
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2381:
RiskId: 73
ComplianceId: 73
RiskTitle: Malware Infection Risk
Criticality: High
PossibleDamage: Data breaches, system compromise, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses, reputational damage
RiskDescription: Failure to deploy anti-virus software may lead to malware infections compromising sy
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular updates and patches for anti-virus software", "2": "Continuous monitoring
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2382:
RiskId: 74
ComplianceId: 74
RiskTitle: Configuration Vulnerability Risk
Criticality: Medium
PossibleDamage: Ineffective malware protection, system vulnerabilities, data breaches
Category: IT
RiskType: Residual
BusinessImpact: System compromise, financial losses, reputational damage
RiskDescription: Improper configuration of anti-virus software may leave systems vulnerable to malwar
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular configuration reviews and updates", "2": "Continuous monitoring of syste
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2383:
RiskId: 75
ComplianceId: 75
RiskTitle: Maintenance Neglect Risk
Criticality: High
PossibleDamage: Outdated malware protection, system vulnerabilities, data breaches

Category: IT
RiskType: Residual
BusinessImpact: System compromise, financial losses, reputational damage
RiskDescription: Failure to maintain and update anti-virus software may lead to outdated protection ag
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Scheduled maintenance and updates for anti-virus software", "2": "Continuous m
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2384:
RiskId: 76
ComplianceId: 76
RiskTitle: Outdated Anti-Virus Software
Criticality: High
PossibleDamage: Increased risk of malware infections and data breaches
Category: IT
RiskType: Residual
BusinessImpact: IT Security Team
RiskDescription: Failure to update anti-virus software exposes systems to known vulnerabilities and in
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate software update process", "2": "Implement real-time monitoring for outd
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2385:
RiskId: 77
ComplianceId: 77
RiskTitle: Undetected Malware Infections
Criticality: High
PossibleDamage: Undetected malware infections leading to data breaches
Category: IT
RiskType: Residual
BusinessImpact: IT Security Team
RiskDescription: Failure to conduct daily malware scans increases the risk of undetected malware infe
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate scan scheduling", "2": "Implement real-time monitoring for scan results"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2386:
RiskId: 78
ComplianceId: 78
RiskTitle: Manual Errors in Update and Scan Management
Criticality: Medium
PossibleDamage: Manual errors in update and scan scheduling leading to security vulnerabilities
Category: IT
RiskType: Residual
BusinessImpact: IT Security Team
RiskDescription: Manual errors in update and scan management can lead to outdated software or miss

RiskLikelihood: 7
RiskImpact: 7
RiskExposureRating: 52.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review automated tool logs", "2": "Implement automated alerts for failed
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2387:
RiskId: 79
ComplianceId: 79
RiskTitle: Lack of Real-time Audit Logs
Criticality: High
PossibleDamage: Undetected security breaches, compromised data integrity
Category: IT
RiskType: Current
BusinessImpact: Potential data loss, reputational damage
RiskDescription: Failure to generate real-time audit logs may result in delayed detection of security inci
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated log generation tools", "2": "Regularly monitor log generation
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2388:
RiskId: 80

ComplianceId: 80
RiskTitle: Insufficient Log Retention Period
Criticality: Medium
PossibleDamage: Loss of historical data for incident investigation and compliance audits
Category: IT
RiskType: Current
BusinessImpact: Inability to track security incidents, compliance violations
RiskDescription: Failure to retain logs for one year may hinder incident response and compliance audit
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement secure storage solutions for logs", "2": "Regularly backup logs to preve
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2389:
RiskId: 81
ComplianceId: 81
RiskTitle: Fragmented Log Storage
Criticality: Medium
PossibleDamage: Inefficiencies in log analysis, delayed incident response
Category: IT
RiskType: Current
BusinessImpact: Inefficient log retrieval, delayed incident response
RiskDescription: Failure to implement centralized logging solutions may lead to fragmented log storage
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement centralized logging tools", "2": "Regularly monitor log storage capacity"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2390:
RiskId: 82
ComplianceId: 82
RiskTitle: Data Breach Due to Unpatched Vulnerabilities
Criticality: High
PossibleDamage: Loss of sensitive data and financial penalties
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, financial losses
RiskDescription: Failure to conduct quarterly vulnerability scans may lead to unpatched vulnerabilities
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement patches promptly", "2": "Regularly update vulnerability scanning tools"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2391:
RiskId: 83
ComplianceId: 83
RiskTitle: Undetected Vulnerabilities Due to Inadequate Scans
Criticality: Medium
PossibleDamage: Data breaches and regulatory fines

Category: IT
RiskType: Residual
BusinessImpact: Reputation damage, financial penalties
RiskDescription: If the IT Security Team fails to conduct vulnerability scans effectively, undetected vuln
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training for IT Security Team on vulnerability scanning best practices", "2
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2392:
RiskId: 84
ComplianceId: 84
RiskTitle: Delayed Detection of Vulnerabilities Post Changes
Criticality: High
PossibleDamage: Exploitation of vulnerabilities post changes
Category: IT
RiskType: Residual
BusinessImpact: Operational disruptions, financial losses
RiskDescription: Failure to conduct scans after significant changes may result in undetected vulnerabil
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement change management process to trigger scans after changes", "2": "Au
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2393:
RiskId: 85
ComplianceId: 85
RiskTitle: High-Risk Vulnerability Remediation Delay
Criticality: High
PossibleDamage: Data breaches, system compromise, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: IT operations, data security
RiskDescription: Failure to remediate high-risk vulnerabilities within the specified timeframe may lead t
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated patch management tools", "2": "Establish clear escalation p
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2394:
RiskId: 86
ComplianceId: 86
RiskTitle: Medium-Risk Vulnerability Remediation Delay
Criticality: Medium
PossibleDamage: Data breaches, system vulnerabilities exploitation
Category: IT
RiskType: Residual
BusinessImpact: IT operations, data security
RiskDescription: Delay in remediating medium-risk vulnerabilities may lead to exploitation by threat act

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated vulnerability management tools", "2": "Regularly update sec
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2395:
RiskId: 87
ComplianceId: 87
RiskTitle: Low-Risk Vulnerability Remediation Delay
Criticality: Low
PossibleDamage: Minor data exposure, limited system impact
Category: IT
RiskType: Residual
BusinessImpact: IT operations, data security
RiskDescription: Failure to remediate low-risk vulnerabilities within the specified timeframe may result i
RiskLikelihood: 4
RiskImpact: 5
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Implement regular security updates", "2": "Enforce security policies and procedure
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2396:
RiskId: 88

ComplianceId: 88
RiskTitle: Data Breach Due to Unpatched Systems
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of business operations, legal consequences
RiskDescription: Failure to apply critical patches promptly may expose systems to exploitation by threa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated patch management tools", "2": "Establish clear patch deplo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2397:
RiskId: 89
ComplianceId: 89
RiskTitle: Ineffective Patch Management System
Criticality: Medium
PossibleDamage: System vulnerabilities, potential data breaches
Category: IT
RiskType: Residual
BusinessImpact: Disruption of business operations, financial losses
RiskDescription: Failure to utilize a patch management system may result in inconsistent patch deploy
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement automated patch deployment processes", "2": "Regularly review and u
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2398:
RiskId: 90
ComplianceId: 90
RiskTitle: Neglected Patch Management Responsibility
Criticality: Low
PossibleDamage: Delayed patch deployment, increased vulnerability exposure
Category: Operational
RiskType: Residual
BusinessImpact: Increased risk of data breaches, compliance violations
RiskDescription: Lack of clear responsibility for patch management may result in delays in patch deplo
RiskLikelihood: 5
RiskImpact: 4
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Establish clear patch management roles and responsibilities", "2": "Provide ongoi
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2399:
RiskId: 91
ComplianceId: 91
RiskTitle: Data Breach Due to Unauthorized Access
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal consequences

Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines, legal liabilities
RiskDescription: Unauthorized access to cardholder data can lead to data breaches and significant fina
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly monitor user access logs",
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2400:
RiskId: 92
ComplianceId: 92
RiskTitle: User Impersonation Due to Shared User IDs
Criticality: Medium
PossibleDamage: Unauthorized access, data manipulation, compliance violations
Category: IT
RiskType: Residual
BusinessImpact: Loss of data integrity, regulatory fines, legal liabilities
RiskDescription: Shared user IDs can lead to user impersonation and unauthorized access to sensitive
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement user ID uniqueness checks", "2": "Enforce user ID expiration policies",
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2401:
RiskId: 93
ComplianceId: 93
RiskTitle: Data Breach Due to Access Control System Vulnerabilities
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines, legal liabilities
RiskDescription: Vulnerabilities in the access control system can lead to unauthorized data access and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update access control system patches", "2": "Implement intrusion detec
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2402:
RiskId: 94
ComplianceId: 94
RiskTitle: Unauthorized Access to Sensitive Areas
Criticality: High
PossibleDamage: Data breaches and compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Facilities Management and Security Personnel
RiskDescription: Unauthorized individuals gaining access to sensitive areas can lead to data breaches

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of access logs", "2": "Employee training on access control procedu
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2403:
RiskId: 95
ComplianceId: 95
RiskTitle: Inconsistent Enforcement of Access Controls
Criticality: Medium
PossibleDamage: Security breaches due to unauthorized access
Category: Operational
RiskType: Residual
BusinessImpact: Facilities Management and Security Personnel
RiskDescription: Intermittent enforcement of access controls can create security vulnerabilities, allowin
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular monitoring of access control systems", "2": "Automated alerts for unautho
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2404:
RiskId: 96

ComplianceId: 96
RiskTitle: Lack of Access Control Log Maintenance
Criticality: Low
PossibleDamage: Difficulty in identifying security incidents
Category: Operational
RiskType: Residual
BusinessImpact: Facilities Management and Security Personnel
RiskDescription: Failure to maintain access control logs can result in the inability to track unauthorized
RiskLikelihood: 4
RiskImpact: 6
RiskExposureRating: 24
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Regular review of access logs", "2": "Automated log retention policies", "3": "Integ
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2405:
RiskId: 97
ComplianceId: 97
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage.
Category: Operational
RiskType: Residual
BusinessImpact: IT Security Team
RiskDescription: Unauthorized individuals gaining access to sensitive cardholder data, leading to poter
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement multi-factor authentication for user access", "2": "Regularly review and

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: IT Operations Unit

Item 2406:

RiskId: 98

ComplianceId: 98

RiskTitle: Loss of User ID Tracking

Criticality: Medium

PossibleDamage: Unauthorized access to cardholder data, compliance violations.

Category: Operational

RiskType: Residual

BusinessImpact: IT Security Team

RiskDescription: Inability to track and manage user IDs effectively, leading to potential unauthorized ac

RiskLikelihood: 5

RiskImpact: 7

RiskExposureRating: 35

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Regularly backup user ID data", "2": "Implement access controls to the user mana

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 2407:

RiskId: 99

ComplianceId: 99

RiskTitle: Unauthorized Access Due to Delayed User ID Assignment

Criticality: High

PossibleDamage: Data breaches, regulatory fines, reputational damage.

Category: Operational
RiskType: Residual
BusinessImpact: IT Security Team
RiskDescription: Delays in assigning user IDs leading to potential unauthorized access to sensitive car
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement user ID assignment workflow", "2": "Automate user ID assignment proc
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2408:
RiskId: 100
ComplianceId: 100
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial repercussions
RiskDescription: Risk of unauthorized access to cardholder data due to weak authentication mechanis
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review access logs", "2": "Implement real-time monitoring for suspicious
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2409:
RiskId: 101
ComplianceId: 101
RiskTitle: Weak Password Risk
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, compromised accounts
RiskDescription: Risk of unauthorized access to cardholder data due to weak password usage.
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement password strength meters", "2": "Provide employee training on passwo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2410:
RiskId: 102
ComplianceId: 102
RiskTitle: Biometric System Failure Risk
Criticality: High
PossibleDamage: Unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, compromised access control
RiskDescription: Risk of unauthorized access due to biometric system failures or compromises.

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement redundant biometric systems", "2": "Regularly test biometric system int
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2411:
RiskId: 103
ComplianceId: 103
RiskTitle: Potential Data Breach Due to Unauthorized Access Events
Criticality: High
PossibleDamage: Data loss, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial liabilities, damage to reputation
RiskDescription: Unauthorized access events may lead to data breaches, exposing sensitive informatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly monitor and review access logs for anomalies", "2": "Implement multi-fa
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2412:
RiskId: 104

ComplianceId: 104
RiskTitle: Undetected Security Incidents Due to Ineffective Audit Trail Review
Criticality: Medium
PossibleDamage: Security incidents, compliance violations, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Compromised system security, regulatory fines, reputational damage
RiskDescription: Failure to review audit trails may result in undetected security incidents or compliance
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish automated alerts for suspicious activities in audit logs", "2": "Conduct re
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2413:
RiskId: 105
ComplianceId: 105
RiskTitle: Tampering of Audit Logs Due to Lack of Encryption
Criticality: High
PossibleDamage: Falsified records, undetected security incidents, compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Loss of data integrity, compromised system security, regulatory fines
RiskDescription: Unencrypted audit logs may be tampered with, leading to falsified records or undetect
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption algorithms for audit log files", "2": "Store encryption l
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2414:
RiskId: 106
ComplianceId: 106
RiskTitle: Failure to Detect Security Incidents
Criticality: High
PossibleDamage: Unauthorized access, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, reputational damage
RiskDescription: Failure to detect security incidents in a timely manner could result in unauthorized acc
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement real-time monitoring tools", "2": "Provide regular training to Security An
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2415:
RiskId: 107
ComplianceId: 107
RiskTitle: Inadequate Log Review Frequency
Criticality: Medium
PossibleDamage: Undetected security incidents, breaches

Category: Operational
RiskType: Residual
BusinessImpact: Data exposure, compliance violations
RiskDescription: Inadequate log review frequency may result in undetected security incidents, data bre
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated log review schedules", "2": "Assign dedicated resources fo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2416:
RiskId: 108
ComplianceId: 108
RiskTitle: Inadequate Utilization of Log Analysis Tools
Criticality: High
PossibleDamage: Undetected anomalies, security incidents
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, compliance violations
RiskDescription: Failure to utilize log analysis tools effectively may result in undetected anomalies, sec
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update log analysis tools", "2": "Provide training on advanced features
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2417:
RiskId: 109
ComplianceId: 109
RiskTitle: Loss of Critical Audit Trail Data
Criticality: High
PossibleDamage: Non-compliance, inability to track security incidents
Category: Operational
RiskType: Current
BusinessImpact: Disruption of compliance processes, potential legal consequences
RiskDescription: Failure to retain audit trail data could result in regulatory fines and compromised secu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular backups of audit trail data", "2": "Encryption of stored logs", "3": "Access
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2418:
RiskId: 110
ComplianceId: 110
RiskTitle: Mismanagement of Audit Trail Data
Criticality: Medium
PossibleDamage: Non-compliance, data integrity issues
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate reporting, potential compliance violations
RiskDescription: Failure to assign responsibility for audit trail retention could lead to mismanagement o

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular audits of compliance officer activities", "2": "Training on retention policies
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2419:
RiskId: 111
ComplianceId: 111
RiskTitle: Outdated Audit Trail Data
Criticality: Medium
PossibleDamage: Missed security incidents, inaccurate reporting
Category: Operational
RiskType: Current
BusinessImpact: Inability to track security incidents, potential compliance violations
RiskDescription: Failure to review and archive audit trails annually could result in outdated data and mi
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated alerts for review deadlines", "2": "Regular training on audit trail review
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2420:
RiskId: 112

ComplianceId: 112
RiskTitle: Undetected Internal Network Vulnerabilities
Criticality: High
PossibleDamage: Increased risk of data breaches and unauthorized access
Category: IT
RiskType: Current
BusinessImpact: Potential loss of sensitive data, reputation damage
RiskDescription: Failure to detect internal network vulnerabilities may result in unauthorized access to
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular internal vulnerability scans", "2": "Address vulnerabilities identi
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2421:
RiskId: 113
ComplianceId: 113
RiskTitle: Undetected External Network Vulnerabilities After Significant Changes
Criticality: Medium
PossibleDamage: Increased risk of data breaches and unauthorized access
Category: IT
RiskType: Current
BusinessImpact: Potential loss of sensitive data, reputation damage
RiskDescription: Failure to detect external network vulnerabilities after significant changes may result i
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement external vulnerability scans after significant changes", "2": "Address vu

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 2422:

RiskId: 114

ComplianceId: 114

RiskTitle: Ineffective Vulnerability Assessments

Criticality: Low

PossibleDamage: Increased risk of undetected vulnerabilities

Category: IT

RiskType: Current

BusinessImpact: Potential exposure to security risks

RiskDescription: Use of ineffective scanning tools and vendors may lead to undetected vulnerabilities a

RiskLikelihood: 5

RiskImpact: 4

RiskExposureRating: 20

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Low

RiskMitigation: {"1": "Regularly review and update approved scanning tools and vendors list", "2": "Con

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 2423:

RiskId: 115

ComplianceId: 115

RiskTitle: Internal Network Vulnerabilities

Criticality: High

PossibleDamage: Data breaches, unauthorized access

Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory fines
RiskDescription: Failure to conduct annual internal penetration testing may leave internal systems vuln
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular internal security assessments", "2": "Implement network monitoring tools"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2424:
RiskId: 116
ComplianceId: 116
RiskTitle: Vulnerabilities Introduced by Changes
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory fines
RiskDescription: Failure to conduct external penetration testing after significant changes may leave sys
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement change control processes", "2": "Perform regular vulnerability scans", "
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2425:
RiskId: 117
ComplianceId: 117
RiskTitle: Incomplete Penetration Testing Methodology
Criticality: High
PossibleDamage: Data breaches, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, regulatory fines
RiskDescription: Failure to develop a comprehensive testing methodology may result in undetected vul
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update testing methodology", "2": "Engage external auditors
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2426:
RiskId: 118
ComplianceId: 118
RiskTitle: Unauthorized Access to Sensitive Data
Criticality: High
PossibleDamage: Data breaches, loss of customer trust
Category: Operational
RiskType: Residual
BusinessImpact: Potential financial losses, reputational damage
RiskDescription: Unauthorized individuals gaining access to sensitive data through unauthorized wirele

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement incident response procedures", "2": "Regularly update wireless detecti
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2427:
RiskId: 119
ComplianceId: 119
RiskTitle: Ineffective Wireless Detection Tools
Criticality: Medium
PossibleDamage: Security breaches, data leaks
Category: IT
RiskType: Residual
BusinessImpact: Loss of sensitive data, reputational damage
RiskDescription: Outdated or ineffective wireless detection tools failing to identify unauthorized access
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a schedule for tool updates", "2": "Test tools after updates to ensure fun
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2428:
RiskId: 120

ComplianceId: 120
RiskTitle: Ineffective Incident Response Procedures
Criticality: High
PossibleDamage: Data breaches, network downtime
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial losses
RiskDescription: Lack of timely and effective response to security incidents involving unauthorized wire
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 68
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly train team members on incident response", "2": "Conduct drills to test re
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2429:
RiskId: 121
ComplianceId: 121
RiskTitle: Outdated Information Security Policy
Criticality: High
PossibleDamage: Increased vulnerability to security breaches and non-compliance with industry stand
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches, financial losses, and reputational damage
RiskDescription: Failure to review the information security policy annually may result in outdated secur
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular policy review meetings with key stakeholders", "2": "Implement tracking s
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2430:
RiskId: 122
ComplianceId: 122
RiskTitle: Outdated Information Security Policy
Criticality: Medium
PossibleDamage: Increased vulnerability to security breaches and non-compliance with industry stand
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches, financial losses, and reputational damage
RiskDescription: Failure to update the information security policy as needed may result in outdated sec
RiskLikelihood: 6
RiskImpact: 6
RiskExposureRating: 39
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear process for policy updates", "2": "Communicate policy changes to
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2431:
RiskId: 123
ComplianceId: 123
RiskTitle: Oversight of Critical Security Requirements
Criticality: High
PossibleDamage: Increased risk of security incidents due to gaps in policy coverage

Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches, financial losses, and reputational damage
RiskDescription: Lack of involvement of key stakeholders in the policy review process may lead to ove
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 68
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish cross-functional review team with representatives from all departments"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2432:
RiskId: 124
ComplianceId: 124
RiskTitle: Failure to Identify Emerging Threats
Criticality: High
PossibleDamage: Data breaches, financial losses, and reputational damage.
Category: Operational
RiskType: Inherent
BusinessImpact: Risk exposure to sensitive data and financial resources.
RiskDescription: Failure to identify emerging threats could result in significant financial and reputationa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular threat intelligence monitoring", "2": "Enhanced security controls impleme
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2433:
RiskId: 125
ComplianceId: 125
RiskTitle: Unidentified Risks from Changes
Criticality: Medium
PossibleDamage: Security incidents, data breaches, and compliance violations.
Category: IT
RiskType: Residual
BusinessImpact: Operational disruptions and financial losses.
RiskDescription: Failure to identify risks introduced by changes could result in operational disruptions a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated change impact analysis tools", "2": "Enhance post-change
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2434:
RiskId: 126
ComplianceId: 126
RiskTitle: Inaccurate Risk Assessments
Criticality: High
PossibleDamage: Inadequate risk mitigation and exposure to critical vulnerabilities.
Category: Compliance
RiskType: Current
BusinessImpact: Non-compliance penalties and reputational damage.
RiskDescription: Inaccurate risk assessments could lead to inadequate risk mitigation, non-compliance

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular validation of assessment results", "2": "Independent review of assessmer
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2435:
RiskId: 127
ComplianceId: 127
RiskTitle: Data Breach Due to Outdated Policies
Criticality: High
PossibleDamage: Data loss, reputational damage, financial losses
Category: Operational
RiskType: Current
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Outdated policies may not address current security threats, leading to vulnerabilities a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Continuous monitoring of policy compli
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2436:
RiskId: 128

ComplianceId: 128
RiskTitle: Unauthorized Access Due to Lack of Awareness
Criticality: Medium
PossibleDamage: Data breaches, unauthorized system access
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, legal implications
RiskDescription: Personnel unaware of usage policies may inadvertently violate security protocols, lea
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training and awareness programs", "2": "Implement access controls", "3":
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2437:
RiskId: 129
ComplianceId: 129
RiskTitle: Data Breach Due to Weak Access Controls
Criticality: High
PossibleDamage: Data loss, reputational damage, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties
RiskDescription: Weak access controls may allow unauthorized individuals to gain access to critical te
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication mechanisms", "2": "Regularly audit access contr
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2438:
RiskId: 130
ComplianceId: 130
RiskTitle: Unauthorized Access to Sensitive Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All departments handling cardholder data would be impacted by unauthorized access
RiskDescription: Unauthorized access to sensitive data can lead to data breaches, financial losses, an
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Regularly review and update access
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2439:
RiskId: 131
ComplianceId: 131
RiskTitle: Role Confusion and Unauthorized Access
Criticality: Medium
PossibleDamage: Confidentiality breaches, data leaks, compliance violations

Category: Operational
RiskType: Residual
BusinessImpact: Role confusion and unauthorized access can lead to confidentiality breaches, data le
RiskDescription: Lack of clarity in role assignments and access control can result in unauthorized acce
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular role reviews and updates", "2": "Implement segregation of duties", "3": "A
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2440:
RiskId: 132
ComplianceId: 132
RiskTitle: Outdated Role Assignments
Criticality: High
PossibleDamage: Increased risk of unauthorized access, compliance gaps, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Outdated role assignments can lead to increased risk of unauthorized access, compli
RiskDescription: Failure to review and update security roles can result in unauthorized access to sensi
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Include role reviews in regular security audits", "2": "Implement automated role re
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2441:
RiskId: 133
ComplianceId: 133
RiskTitle: Phishing Attacks
Criticality: High
PossibleDamage: Loss of sensitive data and financial resources
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Employees unknowingly clicking on malicious links in emails leading to data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement email filtering and security software", "2": "Conduct regular phishing si
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division
Item 2442:
RiskId: 134
ComplianceId: 134
RiskTitle: Social Engineering Attacks
Criticality: Medium
PossibleDamage: Unauthorized access to sensitive information
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: New employees being manipulated into disclosing confidential information to maliciou

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement strict access controls for new employees", "2": "Provide training on rec
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2443:
RiskId: 135
ComplianceId: 135
RiskTitle: Training Content Disengagement
Criticality: Low
PossibleDamage: Reduced effectiveness of security training
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Employees losing interest in training material leading to lower retention of security pra
RiskLikelihood: 4
RiskImpact: 3
RiskExposureRating: 12
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Include interactive elements in e-learning modules", "2": "Gamify training content
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2444:
RiskId: 136

ComplianceId: 136
RiskTitle: Hiring Individuals with False Credentials
Criticality: High
PossibleDamage: Legal consequences, reputational damage, and compromised security
Category: Legal
RiskType: Inherent
BusinessImpact: Potential lawsuits, loss of trust from stakeholders, and security breaches
RiskDescription: If an employee with false credentials is hired, they may not have the necessary qualifi
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify educational and employment history directly with institutions and companie
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2445:
RiskId: 137
ComplianceId: 137
RiskTitle: Misconduct by Existing Employees
Criticality: Medium
PossibleDamage: Reputational damage, legal liabilities, and compromised security
Category: Operational
RiskType: Residual
BusinessImpact: Loss of trust from stakeholders, potential lawsuits, and security breaches
RiskDescription: If an existing employee with a newly acquired criminal record engages in misconduct,
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Conduct regular and thorough background checks on existing employees", "2": "P

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 2446:

RiskId: 138

ComplianceId: 138

RiskTitle: Legal Non-Compliance Due to Missing Documentation

Criticality: Low

PossibleDamage: Legal penalties, challenges in defending hiring decisions, and reputational harm

Category: Legal

RiskType: Inherent

BusinessImpact: Potential fines, legal disputes, and loss of credibility

RiskDescription: If background check findings are not documented, the organization may face legal cha

RiskLikelihood: 4

RiskImpact: 5

RiskExposureRating: 20

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Low

RiskMitigation: {"1": "Implement automated documentation processes for background check findings", "

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 2447:

RiskId: 139

ComplianceId: 139

RiskTitle: Non-Compliance by Service Providers

Criticality: High

PossibleDamage: Data breaches, regulatory fines, reputational damage

Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation, legal consequences
RiskDescription: Failure of service providers to comply with security responsibilities may result in data
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits to verify compliance", "2": "Provide training to service providers on
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2448:
RiskId: 140
ComplianceId: 140
RiskTitle: Legal Non-Compliance by Service Providers
Criticality: Medium
PossibleDamage: Legal disputes, financial penalties, reputational damage
Category: Legal
RiskType: Current
BusinessImpact: Legal disputes, financial penalties, reputational damage
RiskDescription: Failure to include compliance clauses in service provider contracts may result in legal
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Legal review of all contracts to ensure compliance clauses are included", "2": "Re
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2449:
RiskId: 141
ComplianceId: 141
RiskTitle: Gradual Neglect of Security Responsibilities by Service Providers
Criticality: High
PossibleDamage: Data breaches, regulatory fines, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses, damage to reputation, legal consequences
RiskDescription: Failure to conduct annual reviews of service provider agreements may result in servic
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish automated reminders for annual reviews", "2": "Implement regular traini
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2450:
RiskId: 142
ComplianceId: 142
RiskTitle: Data Breach Due to Inadequate Incident Response Procedures
Criticality: High
PossibleDamage: Data exposure, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Inadequate incident response procedures may lead to delays in containment and erad

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training and drills for incident response team", "2": "Continuous monitorin
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2451:
RiskId: 143
ComplianceId: 143
RiskTitle: System Downtime Due to Delayed Incident Response
Criticality: Medium
PossibleDamage: Loss of productivity, financial losses
Category: IT
RiskType: Residual
BusinessImpact: Operational disruptions, revenue loss
RiskDescription: Delayed incident response may lead to prolonged system downtime, impacting busine
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated incident response tools for faster detection and containment", "2": "Re
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2452:
RiskId: 144

ComplianceId: 144
RiskTitle: Ineffective Incident Response Due to Outdated Procedures
Criticality: Low
PossibleDamage: Increased vulnerability to security threats, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Data exposure, regulatory fines
RiskDescription: Outdated incident response procedures may not effectively address current security t
RiskLikelihood: 5
RiskImpact: 4
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Annual review and update of incident response procedures", "2": "Integration of le
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2453:
RiskId: 145
ComplianceId: 145
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: IT, Compliance
RiskDescription: Unauthorized access to cardholder data can result in data breaches and financial loss
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement access controls", "2": "Regular audits of system components", "3": "En
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2454:
RiskId: 146
ComplianceId: 146
RiskTitle: Misidentification of System Components
Criticality: Medium
PossibleDamage: Non-compliance with PCI DSS, security vulnerabilities
Category: Operational
RiskType: Residual
BusinessImpact: IT, Compliance
RiskDescription: Inaccurate network diagrams may lead to misidentification of system components, res
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update network diagrams", "2": "Implement change management proce
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2455:
RiskId: 147
ComplianceId: 147
RiskTitle: Misinterpretation of Data Handling Processes
Criticality: Medium
PossibleDamage: Data leakage, non-compliance with data protection regulations

Category: Operational
RiskType: Residual
BusinessImpact: IT, Compliance
RiskDescription: Inaccurate data flow diagrams may lead to misinterpretation of data handling process
RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update data flow diagrams", "2": "Implement data classification policies"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2456:
RiskId: 148
ComplianceId: 148
RiskTitle: Non-Submission of SAQ
Criticality: High
PossibleDamage: Fines, penalties, suspension of payment processing services
Category: Compliance
RiskType: Residual
BusinessImpact: Financial losses, operational disruptions
RiskDescription: Failure to submit SAQ may lead to non-compliance with payment card industry regula
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict submission deadlines and reminders", "2": "Provide training on a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2457:
RiskId: 149
ComplianceId: 149
RiskTitle: Incomplete ROC Submission
Criticality: Medium
PossibleDamage: Non-compliance fines or penalties
Category: Compliance
RiskType: Residual
BusinessImpact: Financial penalties, reputational damage
RiskDescription: Failure to submit a complete and accurate ROC may lead to non-compliance findings
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear submission guidelines and deadlines", "2": "Conduct internal revie
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2458:
RiskId: 150
ComplianceId: 150
RiskTitle: Inaccurate AOC Attestation
Criticality: High
PossibleDamage: Non-compliance findings and penalties
Category: Compliance
RiskType: Residual
BusinessImpact: Financial penalties, reputational damage
RiskDescription: Inaccurate attestation in the AOC may lead to non-compliance findings and subseque

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Provide training on accurate attestation procedures", "2": "Implement dual verifica
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2459:
RiskId: 151
ComplianceId: 151
RiskTitle: Regulatory Non-Compliance Risk
Criticality: High
PossibleDamage: Financial penalties, reputational harm
Category: Compliance
RiskType: Residual
BusinessImpact: Operational disruptions, legal consequences
RiskDescription: Failure to remediate compliance deficiencies can result in regulatory fines and damag
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Immediate corrective actions", "2": "Thorough documentation of changes", "3": "R
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2460:
RiskId: 152

ComplianceId: 152
RiskTitle: Compliance Reporting Delay Risk
Criticality: Medium
PossibleDamage: Increased regulatory scrutiny, delayed corrective actions
Category: Compliance
RiskType: Residual
BusinessImpact: Operational inefficiencies, compliance audit failures
RiskDescription: Failure to provide timely updates on compliance remediation can result in prolonged r
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting timelines", "2": "Regularly communicate progress update
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2461:
RiskId: 152
ComplianceId: 152
RiskTitle: Compliance Reporting Delay Risk
Criticality: Medium
PossibleDamage: Increased regulatory scrutiny, delayed corrective actions
Category: Compliance
RiskType: Residual
BusinessImpact: Operational inefficiencies, compliance audit failures
RiskDescription: Failure to provide timely updates on compliance remediation can result in prolonged r
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting timelines", "2": "Regularly communicate progress update
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2462:
RiskId: 153
ComplianceId: 153
RiskTitle: Documentation Accuracy Risk
Criticality: High
PossibleDamage: Audit failures, compliance breaches
Category: Compliance
RiskType: Residual
BusinessImpact: Legal consequences, reputational damage
RiskDescription: Inaccurate documentation of compliance changes can result in failed audits and poter
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement robust documentation processes", "2": "Regularly review and update d
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2463:
RiskId: 154
ComplianceId: 157
RiskTitle: Failure to Review Segmentation Methods Annually
Criticality: High
PossibleDamage: Unauthorized access to the CDE, data breaches, non-compliance

Category: Operational
RiskType: Current
BusinessImpact: Disruption of CDE operations, financial losses, reputational damage
RiskDescription: Failure to review segmentation methods annually may result in vulnerabilities being ex
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Schedule regular annual reviews of segmentation methods", "2": "Implement auto
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2464:
RiskId: 154
ComplianceId: 157
RiskTitle: Failure to Review Segmentation Methods Annually
Criticality: High
PossibleDamage: Unauthorized access to the CDE, data breaches, non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Disruption of CDE operations, financial losses, reputational damage
RiskDescription: Failure to review segmentation methods annually may result in vulnerabilities being ex
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Schedule regular annual reviews of segmentation methods", "2": "Implement auto
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2465:
RiskId: 155
ComplianceId: 158
RiskTitle: Lack of Documentation for Segmentation Configurations
Criticality: Medium
PossibleDamage: Misconfigurations, mismanagement, security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of security incidents, potential data breaches, compliance violations
RiskDescription: Failure to maintain detailed documentation of segmentation configurations may result
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a centralized repository for storing segmentation documentation", "2":
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2466:
RiskId: 155
ComplianceId: 158
RiskTitle: Lack of Documentation for Segmentation Configurations
Criticality: Medium
PossibleDamage: Misconfigurations, mismanagement, security vulnerabilities
Category: Operational
RiskType: Current
BusinessImpact: Increased risk of security incidents, potential data breaches, compliance violations
RiskDescription: Failure to maintain detailed documentation of segmentation configurations may result

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement a centralized repository for storing segmentation documentation", "2":
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2467:
RiskId: 156
ComplianceId: 159
RiskTitle: Lack of Network Monitoring for Segmentation
Criticality: High
PossibleDamage: Undetected security incidents, data breaches, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Data breaches, financial losses, reputational damage
RiskDescription: Failure to utilize network monitoring tools for segmentation may result in undetected s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement continuous monitoring of network traffic for anomalies", "2": "Set up ale
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2468:
RiskId: 156

ComplianceId: 159
RiskTitle: Lack of Network Monitoring for Segmentation
Criticality: High
PossibleDamage: Undetected security incidents, data breaches, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Data breaches, financial losses, reputational damage
RiskDescription: Failure to utilize network monitoring tools for segmentation may result in undetected s
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement continuous monitoring of network traffic for anomalies", "2": "Set up ale
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2469:
RiskId: 157
ComplianceId: 160
RiskTitle: Non-Compliant Third-Party Providers
Criticality: High
PossibleDamage: Data breaches, financial penalties, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, loss of customer trust
RiskDescription: Failure to verify third-party compliance can lead to serious consequences for the orga
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular audits of third-party compliance", "2": "Strong contractual obligations for c
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2470:
RiskId: 157
ComplianceId: 160
RiskTitle: Non-Compliant Third-Party Providers
Criticality: High
PossibleDamage: Data breaches, financial penalties, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Disruption of operations, financial losses, loss of customer trust
RiskDescription: Failure to verify third-party compliance can lead to serious consequences for the orga
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of third-party compliance", "2": "Strong contractual obligations for c
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2471:
RiskId: 158
ComplianceId: 161
RiskTitle: Non-Compliant New Providers
Criticality: High
PossibleDamage: Immediate data breaches, financial penalties, reputational damage

Category: Compliance
RiskType: Current
BusinessImpact: Immediate disruption of operations, financial losses, loss of customer trust
RiskDescription: Failure to verify compliance of new providers can have immediate detrimental effects
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Thorough due diligence before engagement", "2": "Compliance checks in vendor
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2472:
RiskId: 159
ComplianceId: 162
RiskTitle: Lack of Oversight in Third-Party Relationships
Criticality: High
PossibleDamage: Compliance breaches, data breaches, financial penalties
Category: Compliance
RiskType: Current
BusinessImpact: Legal consequences, financial losses, reputational damage
RiskDescription: Inadequate oversight of third-party relationships can result in serious compliance and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 77.2
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear oversight processes and responsibilities", "2": "Regularly review th
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2473:
RiskId: 159
ComplianceId: 162
RiskTitle: Lack of Oversight in Third-Party Relationships
Criticality: High
PossibleDamage: Compliance breaches, data breaches, financial penalties
Category: Compliance
RiskType: Current
BusinessImpact: Legal consequences, financial losses, reputational damage
RiskDescription: Inadequate oversight of third-party relationships can result in serious compliance and
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 77.2
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear oversight processes and responsibilities", "2": "Regularly review th
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2474:
RiskId: 160
ComplianceId: 163
RiskTitle: Non-compliance with Annual SAQ Completion
Criticality: High
PossibleDamage: Fines, reputational damage, data breaches
Category: Compliance
RiskType: Current
BusinessImpact: Potential financial losses, reputational damage, and legal consequences
RiskDescription: Failure to complete the SAQ annually may result in non-compliance with PCI DSS sta

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely completion of the SAQ by setting reminders and deadlines", "2": "R
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2475:
RiskId: 160
ComplianceId: 163
RiskTitle: Non-compliance with Annual SAQ Completion
Criticality: High
PossibleDamage: Fines, reputational damage, data breaches
Category: Compliance
RiskType: Current
BusinessImpact: Potential financial losses, reputational damage, and legal consequences
RiskDescription: Failure to complete the SAQ annually may result in non-compliance with PCI DSS sta
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely completion of the SAQ by setting reminders and deadlines", "2": "R
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2476:
RiskId: 160

ComplianceId: 163
RiskTitle: Non-compliance with Annual SAQ Completion
Criticality: High
PossibleDamage: Fines, reputational damage, data breaches
Category: Compliance
RiskType: Current
BusinessImpact: Potential financial losses, reputational damage, and legal consequences
RiskDescription: Failure to complete the SAQ annually may result in non-compliance with PCI DSS sta
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Ensure timely completion of the SAQ by setting reminders and deadlines", "2": "R
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2477:
RiskId: 161
ComplianceId: 164
RiskTitle: Loss of Documentation
Criticality: Medium
PossibleDamage: Inability to prove compliance, fines, penalties
Category: Operational
RiskType: Current
BusinessImpact: Loss of compliance status, financial penalties
RiskDescription: Loss of documentation related to SAQ completion and remediation plans may result i
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement secure document storage procedures", "2": "Regularly backup docume
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2478:
RiskId: 161
ComplianceId: 164
RiskTitle: Loss of Documentation
Criticality: Medium
PossibleDamage: Inability to prove compliance, fines, penalties
Category: Operational
RiskType: Current
BusinessImpact: Loss of compliance status, financial penalties
RiskDescription: Loss of documentation related to SAQ completion and remediation plans may result i
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement secure document storage procedures", "2": "Regularly backup docume
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2479:
RiskId: 161
ComplianceId: 164
RiskTitle: Loss of Documentation
Criticality: Medium
PossibleDamage: Inability to prove compliance, fines, penalties

Category: Operational
RiskType: Current
BusinessImpact: Loss of compliance status, financial penalties
RiskDescription: Loss of documentation related to SAQ completion and remediation plans may result i
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement secure document storage procedures", "2": "Regularly backup docume
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2480:
RiskId: 162
ComplianceId: 165
RiskTitle: Failure to Document Remediation Plans
Criticality: High
PossibleDamage: Unresolved compliance issues, potential data breaches
Category: Compliance
RiskType: Current
BusinessImpact: Impact on security posture, reputation
RiskDescription: Failure to document remediation plans for addressing 'no' answers in the SAQ may re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear guidelines for documenting remediation plans", "2": "Review and a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2481:
RiskId: 162
ComplianceId: 165
RiskTitle: Failure to Document Remediation Plans
Criticality: High
PossibleDamage: Unresolved compliance issues, potential data breaches
Category: Compliance
RiskType: Current
BusinessImpact: Impact on security posture, reputation
RiskDescription: Failure to document remediation plans for addressing 'no' answers in the SAQ may re
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear guidelines for documenting remediation plans", "2": "Review and a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2482:
RiskId: 162
ComplianceId: 165
RiskTitle: Failure to Document Remediation Plans
Criticality: High
PossibleDamage: Unresolved compliance issues, potential data breaches
Category: Compliance
RiskType: Current
BusinessImpact: Impact on security posture, reputation
RiskDescription: Failure to document remediation plans for addressing 'no' answers in the SAQ may re

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear guidelines for documenting remediation plans", "2": "Review and a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2483:
RiskId: 163
ComplianceId: 169
RiskTitle: Non-Submission of RoC
Criticality: High
PossibleDamage: Non-compliance penalties, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Financial losses, legal consequences
RiskDescription: Failure to submit the RoC may lead to regulatory fines and damage to the organizatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear submission timelines and responsibilities", "2": "Implement regular
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2484:
RiskId: 163

ComplianceId: 169
RiskTitle: Non-Submission of RoC
Criticality: High
PossibleDamage: Non-compliance penalties, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Financial losses, legal consequences
RiskDescription: Failure to submit the RoC may lead to regulatory fines and damage to the organizatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear submission timelines and responsibilities", "2": "Implement regular
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2485:
RiskId: 163
ComplianceId: 169
RiskTitle: Non-Submission of RoC
Criticality: High
PossibleDamage: Non-compliance penalties, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Financial losses, legal consequences
RiskDescription: Failure to submit the RoC may lead to regulatory fines and damage to the organizatio
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear submission timelines and responsibilities", "2": "Implement regular
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2486:
RiskId: 164
ComplianceId: 170
RiskTitle: Outdated Scan Results
Criticality: Medium
PossibleDamage: Undetected vulnerabilities, non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, financial losses
RiskDescription: Failure to update scan results may result in undetected vulnerabilities and potential no
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate scan result updates", "2": "Implement regular review processes", "3": "T
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2487:
RiskId: 164
ComplianceId: 170
RiskTitle: Outdated Scan Results
Criticality: Medium
PossibleDamage: Undetected vulnerabilities, non-compliance

Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, financial losses
RiskDescription: Failure to update scan results may result in undetected vulnerabilities and potential no
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate scan result updates", "2": "Implement regular review processes", "3": "T
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2488:
RiskId: 164
ComplianceId: 170
RiskTitle: Outdated Scan Results
Criticality: Medium
PossibleDamage: Undetected vulnerabilities, non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, financial losses
RiskDescription: Failure to update scan results may result in undetected vulnerabilities and potential no
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate scan result updates", "2": "Implement regular review processes", "3": "T
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2489:
RiskId: 165
ComplianceId: 171
RiskTitle: Missing Executive Summary
Criticality: Low
PossibleDamage: Misinterpretation of compliance status and findings
Category: Operational
RiskType: Residual
BusinessImpact: Miscommunication, compliance misunderstandings
RiskDescription: Failure to include an executive summary may lead to stakeholders misinterpreting cor
RiskLikelihood: 5
RiskImpact: 3
RiskExposureRating: 15
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Standardize executive summary inclusion process", "2": "Implement review mecha
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2490:
RiskId: 165
ComplianceId: 171
RiskTitle: Missing Executive Summary
Criticality: Low
PossibleDamage: Misinterpretation of compliance status and findings
Category: Operational
RiskType: Residual
BusinessImpact: Miscommunication, compliance misunderstandings
RiskDescription: Failure to include an executive summary may lead to stakeholders misinterpreting cor

RiskLikelihood: 5
RiskImpact: 3
RiskExposureRating: 15
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Standardize executive summary inclusion process", "2": "Implement review mecha
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2491:
RiskId: 166
ComplianceId: 172
RiskTitle: Lack of Continuous Monitoring
Criticality: High
PossibleDamage: Increased risk of security breaches and non-compliance penalties
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses and damage to organizational reputation
RiskDescription: Failure to monitor security controls could result in undetected vulnerabilities and non-c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools", "2": "Regularly review monitoring reports"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2492:
RiskId: 166

ComplianceId: 172
RiskTitle: Lack of Continuous Monitoring
Criticality: High
PossibleDamage: Increased risk of security breaches and non-compliance penalties
Category: Operational
RiskType: Current
BusinessImpact: Potential financial losses and damage to organizational reputation
RiskDescription: Failure to monitor security controls could result in undetected vulnerabilities and non-
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools", "2": "Regularly review monitoring reports"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2493:
RiskId: 167
ComplianceId: 173
RiskTitle: Inadequate Quarterly Reviews
Criticality: Medium
PossibleDamage: Failure to identify non-compliance issues and address security gaps
Category: Operational
RiskType: Current
BusinessImpact: Potential non-compliance penalties and compromised security posture
RiskDescription: Lack of quarterly reviews may lead to unidentified compliance issues and security vul
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish formal review procedures", "2": "Document review findings and action it
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2494:
RiskId: 167
ComplianceId: 173
RiskTitle: Inadequate Quarterly Reviews
Criticality: Medium
PossibleDamage: Failure to identify non-compliance issues and address security gaps
Category: Operational
RiskType: Current
BusinessImpact: Potential non-compliance penalties and compromised security posture
RiskDescription: Lack of quarterly reviews may lead to unidentified compliance issues and security vul
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish formal review procedures", "2": "Document review findings and action it
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2495:
RiskId: 168
ComplianceId: 174
RiskTitle: Absence of Compliance Calendar
Criticality: Medium
PossibleDamage: Missed compliance deadlines and lack of visibility into compliance activities

Category: Operational
RiskType: Current
BusinessImpact: Potential non-compliance penalties and operational disruptions
RiskDescription: Without a compliance calendar, there is a risk of missing deadlines and incomplete co
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop a detailed compliance calendar", "2": "Assign responsibilities for complia
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2496:
RiskId: 168
ComplianceId: 174
RiskTitle: Absence of Compliance Calendar
Criticality: Medium
PossibleDamage: Missed compliance deadlines and lack of visibility into compliance activities
Category: Operational
RiskType: Current
BusinessImpact: Potential non-compliance penalties and operational disruptions
RiskDescription: Without a compliance calendar, there is a risk of missing deadlines and incomplete co
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop a detailed compliance calendar", "2": "Assign responsibilities for complia
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2497:
RiskId: 169
ComplianceId: 175
RiskTitle: Outdated Knowledge of PCI DSS Requirements
Criticality: High
PossibleDamage: Potential security vulnerabilities and non-compliance with PCI DSS
Category: Operational
RiskType: Residual
BusinessImpact: Finance, Operations
RiskDescription: Personnel may not be aware of the latest PCI DSS requirements, leading to security v
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training sessions on PCI DSS updates", "2": "Internal audits to verify com
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2498:
RiskId: 170
ComplianceId: 176
RiskTitle: Lack of Training Completion Documentation
Criticality: Medium
PossibleDamage: Non-compliance with internal training requirements and potential knowledge gaps
Category: Operational
RiskType: Residual
BusinessImpact: HR, Compliance
RiskDescription: Failure to document training completion may result in non-compliance with internal re

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated tracking system for training completion", "2": "Regular reporting to con
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2499:
RiskId: 170
ComplianceId: 176
RiskTitle: Lack of Training Completion Documentation
Criticality: Medium
PossibleDamage: Non-compliance with internal training requirements and potential knowledge gaps
Category: Operational
RiskType: Residual
BusinessImpact: HR, Compliance
RiskDescription: Failure to document training completion may result in non-compliance with internal re
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated tracking system for training completion", "2": "Regular reporting to con
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2500:
RiskId: 171

ComplianceId: 177
RiskTitle: Lack of Access to Relevant Resources
Criticality: Low
PossibleDamage: Outdated knowledge and inefficient processes
Category: Operational
RiskType: Residual
BusinessImpact: IT, Training
RiskDescription: Without access to relevant resources, personnel may lack updated knowledge and ma
RiskLikelihood: 4
RiskImpact: 5
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Regular communication on available resources", "2": "Training needs assessment
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2501:
RiskId: 171
ComplianceId: 177
RiskTitle: Lack of Access to Relevant Resources
Criticality: Low
PossibleDamage: Outdated knowledge and inefficient processes
Category: Operational
RiskType: Residual
BusinessImpact: IT, Training
RiskDescription: Without access to relevant resources, personnel may lack updated knowledge and ma
RiskLikelihood: 4
RiskImpact: 5
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Low
RiskMitigation: {"1": "Regular communication on available resources", "2": "Training needs assessment
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2502:
RiskId: 172
ComplianceId: 178
RiskTitle: Non-Completion of PCI Awareness Training
Criticality: High
PossibleDamage: Potential data breaches, financial penalties, and reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial losses, and regulatory fines
RiskDescription: Failure to complete PCI awareness training may result in staff not understanding secu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reminders and notifications to staff about training deadlines", "2": "Provid
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2503:
RiskId: 172
ComplianceId: 178
RiskTitle: Non-Completion of PCI Awareness Training
Criticality: High
PossibleDamage: Potential data breaches, financial penalties, and reputational damage

Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial losses, and regulatory fines
RiskDescription: Failure to complete PCI awareness training may result in staff not understanding secu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular reminders and notifications to staff about training deadlines", "2": "Provid
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2504:
RiskId: 173
ComplianceId: 179
RiskTitle: Inadequate PCI Training Content
Criticality: Medium
PossibleDamage: Data breaches, non-compliance with PCI DSS, and financial losses
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial penalties, and reputational damage
RiskDescription: If the training content does not adequately cover PCI DSS requirements and security
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update training content to align with current PCI DSS requir
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2505:
RiskId: 174
ComplianceId: 180
RiskTitle: Lack of Training Compliance Monitoring
Criticality: High
PossibleDamage: Non-compliance with PCI DSS, audit failures, and financial penalties
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial losses, and reputational damage
RiskDescription: Without consistent monitoring of training compliance and accurate record-keeping, no
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated tracking systems for training completion", "2": "Regularly re
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2506:
RiskId: 174
ComplianceId: 180
RiskTitle: Lack of Training Compliance Monitoring
Criticality: High
PossibleDamage: Non-compliance with PCI DSS, audit failures, and financial penalties
Category: Operational
RiskType: Current
BusinessImpact: Loss of customer trust, financial losses, and reputational damage
RiskDescription: Without consistent monitoring of training compliance and accurate record-keeping, no

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated tracking systems for training completion", "2": "Regularly re
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2507:
RiskId: 175
ComplianceId: 181
RiskTitle: Data Breach Due to Non-Compliance
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal penalties
Category: Compliance
RiskType: Current
BusinessImpact: Finance, IT, Operations
RiskDescription: Unauthorized use of non-approved products could lead to a data breach compromisin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on approved products", "2": "Strict monitoring of product usage",
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2508:
RiskId: 175

ComplianceId: 181
RiskTitle: Data Breach Due to Non-Compliance
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal penalties
Category: Compliance
RiskType: Current
BusinessImpact: Finance, IT, Operations
RiskDescription: Unauthorized use of non-approved products could lead to a data breach compromisin
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training on approved products", "2": "Strict monitoring of product usage",
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2509:
RiskId: 176
ComplianceId: 182
RiskTitle: Non-Compliance During Annual Audit
Criticality: Medium
PossibleDamage: Compliance violations, penalties, reputational damage
Category: Compliance
RiskType: Current
BusinessImpact: Finance, IT, Operations
RiskDescription: Failure to comply during the annual audit could lead to penalties and reputational dam
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regular internal audits throughout the year", "2": "Proactive remediation of any no
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2510:
RiskId: 177
ComplianceId: 183
RiskTitle: Delayed Reporting of Non-Compliance
Criticality: Low
PossibleDamage: Increased risk exposure, potential breaches
Category: Compliance
RiskType: Current
BusinessImpact: Finance, IT, Operations
RiskDescription: Failure to report non-compliance issues promptly could increase the risk exposure an
RiskLikelihood: 5
RiskImpact: 3
RiskExposureRating: 15
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Clear reporting procedures and channels", "2": "Regular training on reporting requ
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2511:
RiskId: 177
ComplianceId: 183
RiskTitle: Delayed Reporting of Non-Compliance
Criticality: Low
PossibleDamage: Increased risk exposure, potential breaches

Category: Compliance
RiskType: Current
BusinessImpact: Finance, IT, Operations
RiskDescription: Failure to report non-compliance issues promptly could increase the risk exposure an
RiskLikelihood: 5
RiskImpact: 3
RiskExposureRating: 15
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Clear reporting procedures and channels", "2": "Regular training on reporting requ
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2512:
RiskId: 178
ComplianceId: 184
RiskTitle: Data Breach Due to Outdated Firewall Configuration
Criticality: High
PossibleDamage: Loss of sensitive cardholder data, financial penalties, reputational damage.
Category: Operational
RiskType: Residual
BusinessImpact: Financial loss, Legal consequences
RiskDescription: Failure to review firewall configurations quarterly may result in vulnerabilities that coul
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools", "2": "Enforce strict change control proced
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2513:
RiskId: 178
ComplianceId: 184
RiskTitle: Data Breach Due to Outdated Firewall Configuration
Criticality: High
PossibleDamage: Loss of sensitive cardholder data, financial penalties, reputational damage.
Category: Operational
RiskType: Residual
BusinessImpact: Financial loss, Legal consequences
RiskDescription: Failure to review firewall configurations quarterly may result in vulnerabilities that coul
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated monitoring tools", "2": "Enforce strict change control proced
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2514:
RiskId: 179
ComplianceId: 185
RiskTitle: Network Vulnerabilities Due to Poor Documentation
Criticality: Medium
PossibleDamage: Unauthorized access, Data breaches, Compliance fines.
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions, Legal consequences
RiskDescription: Incomplete or outdated documentation of firewall rule sets may lead to misconfiguratio

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement documentation management system", "2": "Regularly review and upda
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2515:
RiskId: 179
ComplianceId: 185
RiskTitle: Network Vulnerabilities Due to Poor Documentation
Criticality: Medium
PossibleDamage: Unauthorized access, Data breaches, Compliance fines.
Category: Operational
RiskType: Residual
BusinessImpact: Operational disruptions, Legal consequences
RiskDescription: Incomplete or outdated documentation of firewall rule sets may lead to misconfiguratio
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement documentation management system", "2": "Regularly review and upda
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2516:
RiskId: 180

ComplianceId: 186
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, Financial loss, Legal consequences.
Category: Operational
RiskType: Residual
BusinessImpact: Financial loss, Legal consequences
RiskDescription: Failure to review and update access controls may result in unauthorized access to se
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement role-based access controls", "2": "Regularly review access permission
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2517:
RiskId: 180
ComplianceId: 186
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, Financial loss, Legal consequences.
Category: Operational
RiskType: Residual
BusinessImpact: Financial loss, Legal consequences
RiskDescription: Failure to review and update access controls may result in unauthorized access to se
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement role-based access controls", "2": "Regularly review access permission
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2518:
RiskId: 181
ComplianceId: 187
RiskTitle: Unauthorized Access Due to Default Passwords
Criticality: High
PossibleDamage: Unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Potential loss of sensitive information
RiskDescription: Failure to change default passwords could lead to unauthorized access to systems ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Enforce regular password changes", "3
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2519:
RiskId: 181
ComplianceId: 187
RiskTitle: Unauthorized Access Due to Default Passwords
Criticality: High
PossibleDamage: Unauthorized access, data breaches

Category: IT
RiskType: Residual
BusinessImpact: Potential loss of sensitive information
RiskDescription: Failure to change default passwords could lead to unauthorized access to systems ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong password policies", "2": "Enforce regular password changes", "3
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2520:
RiskId: 182
ComplianceId: 188
RiskTitle: Lack of Documentation for Default Settings Changes
Criticality: Medium
PossibleDamage: Confusion, errors, security vulnerabilities
Category: Operational
RiskType: Residual
BusinessImpact: Potential errors in system configurations
RiskDescription: Failure to document default settings changes could lead to confusion, errors, and pote
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement documentation procedures", "2": "Regularly review and update docum
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma

CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2521:
RiskId: 182
ComplianceId: 188
RiskTitle: Lack of Documentation for Default Settings Changes
Criticality: Medium
PossibleDamage: Confusion, errors, security vulnerabilities
Category: Operational
RiskType: Residual
BusinessImpact: Potential errors in system configurations
RiskDescription: Failure to document default settings changes could lead to confusion, errors, and pote
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement documentation procedures", "2": "Regularly review and update docum
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2522:
RiskId: 183
ComplianceId: 189
RiskTitle: Outdated Default Settings Due to Lack of Annual Review
Criticality: Medium
PossibleDamage: Security vulnerabilities, breaches
Category: IT
RiskType: Residual
BusinessImpact: Potential breaches due to outdated security measures
RiskDescription: Failure to review default settings annually could lead to outdated security measures a

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 45.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Schedule annual reviews", "2": "Implement change management process for defa
CreatedAt: 2025-10-07 00:00:00
CreatedBy: radha.sharma
CreatedByName: Radha Sharma
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2523:
RiskId: 184
ComplianceId: 190
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive cardholder data
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Risk of unauthorized access to stored cardholder data leading to data breaches and f
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption algorithms to industry standards", "2": "Implement ac
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2524:
RiskId: 184

ComplianceId: 190
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive cardholder data
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Risk of unauthorized access to stored cardholder data leading to data breaches and f
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption algorithms to industry standards", "2": "Implement ac
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2525:
RiskId: 185
ComplianceId: 191
RiskTitle: Encryption Implementation Risk
Criticality: Medium
PossibleDamage: Inconsistent or ineffective encryption implementation
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, regulatory fines
RiskDescription: Risk of inconsistent or ineffective encryption implementation leading to data breaches
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Provide regular training to the data security team on encryption best practices", "2
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2526:
RiskId: 185
ComplianceId: 191
RiskTitle: Encryption Implementation Risk
Criticality: Medium
PossibleDamage: Inconsistent or ineffective encryption implementation
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, regulatory fines
RiskDescription: Risk of inconsistent or ineffective encryption implementation leading to data breaches
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide regular training to the data security team on encryption best practices", "2
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2527:
RiskId: 186
ComplianceId: 192
RiskTitle: Encryption Review Risk
Criticality: Low
PossibleDamage: Outdated encryption methods

Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, non-compliance penalties
RiskDescription: Risk of using outdated encryption methods leading to data breaches and non-compli
RiskLikelihood: 4
RiskImpact: 5
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Schedule regular encryption reviews and updates", "2": "Implement automated en
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2528:
RiskId: 186
ComplianceId: 192
RiskTitle: Encryption Review Risk
Criticality: Low
PossibleDamage: Outdated encryption methods
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, non-compliance penalties
RiskDescription: Risk of using outdated encryption methods leading to data breaches and non-compli
RiskLikelihood: 4
RiskImpact: 5
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Schedule regular encryption reviews and updates", "2": "Implement automated en
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel

CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2529:
RiskId: 187
ComplianceId: 193
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches leading to financial losses and reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust and potential legal consequences
RiskDescription: Unauthorized access to cardholder data during transmission can result in financial los
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption protocols", "2": "Regularly monitor network traffic for
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2530:
RiskId: 187
ComplianceId: 193
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches leading to financial losses and reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust and potential legal consequences
RiskDescription: Unauthorized access to cardholder data during transmission can result in financial los

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption protocols", "2": "Regularly monitor network traffic for
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2531:
RiskId: 188
ComplianceId: 194
RiskTitle: Outdated Encryption Protocols
Criticality: Medium
PossibleDamage: Data breaches and loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust and potential regulatory fines
RiskDescription: Outdated encryption protocols can expose cardholder data to unauthorized access, le
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update encryption protocols based on industry standards", "2": "Conduc
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2532:
RiskId: 188

ComplianceId: 194
RiskTitle: Outdated Encryption Protocols
Criticality: Medium
PossibleDamage: Data breaches and loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust and potential regulatory fines
RiskDescription: Outdated encryption protocols can expose cardholder data to unauthorized access, le
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update encryption protocols based on industry standards", "2": "Conduc
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2533:
RiskId: 189
ComplianceId: 195
RiskTitle: Data Interception of Cardholder Data
Criticality: High
PossibleDamage: Unauthorized access to sensitive cardholder data
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust and potential legal consequences
RiskDescription: Data interception during transmission can lead to unauthorized access to cardholder
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption protocols", "2": "Regularly monitor network traffic for
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2534:
RiskId: 189
ComplianceId: 195
RiskTitle: Data Interception of Cardholder Data
Criticality: High
PossibleDamage: Unauthorized access to sensitive cardholder data
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust and potential legal consequences
RiskDescription: Data interception during transmission can lead to unauthorized access to cardholder d
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong encryption protocols", "2": "Regularly monitor network traffic for
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2535:
RiskId: 190
ComplianceId: 196
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data breaches, financial losses

Category: IT
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Unauthorized access to cardholder data due to insecure coding practices.
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implementing secure coding guidelines", "2": "Regular code reviews", "3": "Securi
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2536:
RiskId: 190
ComplianceId: 196
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: IT
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Unauthorized access to cardholder data due to insecure coding practices.
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implementing secure coding guidelines", "2": "Regular code reviews", "3": "Securi
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel

CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2537:
RiskId: 191
ComplianceId: 197
RiskTitle: Application Vulnerability Risk
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Undetected vulnerabilities in applications due to lack of security reviews.
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing security checkpoints", "2": "Regular security audits", "3": "Continuou
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2538:
RiskId: 191
ComplianceId: 197
RiskTitle: Application Vulnerability Risk
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Undetected vulnerabilities in applications due to lack of security reviews.

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implementing security checkpoints", "2": "Regular security audits", "3": "Continuou
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2539:
RiskId: 192
ComplianceId: 198
RiskTitle: Automated Testing Tool Failure Risk
Criticality: High
PossibleDamage: Unidentified vulnerabilities, security breaches
Category: IT
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Failure of automated security testing tools to detect vulnerabilities in applications.
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Integrating tools in CI/CD pipeline", "2": "Regular updates and maintenance", "3":
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2540:
RiskId: 192

ComplianceId: 198
RiskTitle: Automated Testing Tool Failure Risk
Criticality: High
PossibleDamage: Unidentified vulnerabilities, security breaches
Category: IT
RiskType: Residual
BusinessImpact: Financial losses, reputational damage
RiskDescription: Failure of automated security testing tools to detect vulnerabilities in applications.
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Integrating tools in CI/CD pipeline", "2": "Regular updates and maintenance", "3":
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2541:
RiskId: 193
ComplianceId: 199
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: Unauthorized access to cardholder data can lead to data breaches, financial losses, a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access permissions", "2": "Provide training on role-b
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2542:
RiskId: 193
ComplianceId: 199
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: Unauthorized access to cardholder data can lead to data breaches, financial losses, a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access permissions", "2": "Provide training on role-b
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2543:
RiskId: 194
ComplianceId: 200
RiskTitle: Outdated Access Permissions
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches

Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: Outdated access permissions can lead to unauthorized access to cardholder data, po
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate access permission reviews", "2": "Implement access permission change
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2544:
RiskId: 194
ComplianceId: 200
RiskTitle: Outdated Access Permissions
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: Outdated access permissions can lead to unauthorized access to cardholder data, po
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate access permission reviews", "2": "Implement access permission change
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel

CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2545:
RiskId: 195
ComplianceId: 201
RiskTitle: Inaccurate Access Control List
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: An inaccurate access control list can lead to unauthorized access to cardholder data,
RiskLikelihood: 7
RiskImpact: 7
RiskExposureRating: 52.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update access control list", "2": "Implement access control list change n
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2546:
RiskId: 195
ComplianceId: 201
RiskTitle: Inaccurate Access Control List
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: An inaccurate access control list can lead to unauthorized access to cardholder data,

RiskLikelihood: 7
RiskImpact: 7
RiskExposureRating: 52.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly update access control list", "2": "Implement access control list change m
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2547:
RiskId: 196
ComplianceId: 202
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Potential compromise of sensitive data and financial losses.
RiskDescription: Unauthorized access to system components can lead to data breaches and financial l
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement biometric authentication for added security", "2": "Regularly review and
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2548:
RiskId: 196

ComplianceId: 202
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Potential compromise of sensitive data and financial losses.
RiskDescription: Unauthorized access to system components can lead to data breaches and financial l
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement biometric authentication for added security", "2": "Regularly review and
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2549:
RiskId: 197
ComplianceId: 203
RiskTitle: Outdated Authentication Risk
Criticality: Medium
PossibleDamage: Increased risk of unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Potential compromise of sensitive data and security breaches.
RiskDescription: Outdated authentication methods can lead to increased risk of unauthorized access a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Conduct regular audits of authentication logs", "2": "Implement automated alerts f
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2550:
RiskId: 197
ComplianceId: 203
RiskTitle: Outdated Authentication Risk
Criticality: Medium
PossibleDamage: Increased risk of unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Potential compromise of sensitive data and security breaches.
RiskDescription: Outdated authentication methods can lead to increased risk of unauthorized access a
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Conduct regular audits of authentication logs", "2": "Implement automated alerts f
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2551:
RiskId: 198
ComplianceId: 204
RiskTitle: User Identification Risk
Criticality: High
PossibleDamage: Unauthorized access, data breaches

Category: IT
RiskType: Residual
BusinessImpact: Potential compromise of sensitive data and security breaches.
RiskDescription: Lack of unique user identification may lead to unauthorized access and data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement user account management policies", "2": "Enforce strong password rec
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2552:
RiskId: 198
ComplianceId: 204
RiskTitle: User Identification Risk
Criticality: High
PossibleDamage: Unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Potential compromise of sensitive data and security breaches.
RiskDescription: Lack of unique user identification may lead to unauthorized access and data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement user account management policies", "2": "Enforce strong password rec
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel

CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2553:
RiskId: 199
ComplianceId: 205
RiskTitle: Delayed Access Log Review
Criticality: High
PossibleDamage: Unauthorized access or data breaches
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of sensitive data, reputation damage
RiskDescription: Failure to review access logs daily may lead to undetected unauthorized access or da
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate access log review process", "2": "Implement alerts for suspicious acces
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2554:
RiskId: 199
ComplianceId: 205
RiskTitle: Delayed Access Log Review
Criticality: High
PossibleDamage: Unauthorized access or data breaches
Category: Operational
RiskType: Current
BusinessImpact: Potential loss of sensitive data, reputation damage
RiskDescription: Failure to review access logs daily may lead to undetected unauthorized access or da

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate access log review process", "2": "Implement alerts for suspicious acces
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2555:
RiskId: 200
ComplianceId: 206
RiskTitle: Non-Compliance with Data Retention Regulations
Criticality: Medium
PossibleDamage: Penalties for non-compliance, inability to track historical access
Category: Operational
RiskType: Current
BusinessImpact: Legal consequences, compromised historical access tracking
RiskDescription: Failure to retain access logs for the required period may result in regulatory penalties
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated data retention policies", "2": "Regularly audit access log ret
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2556:
RiskId: 200

ComplianceId: 206
RiskTitle: Non-Compliance with Data Retention Regulations
Criticality: Medium
PossibleDamage: Penalties for non-compliance, inability to track historical access
Category: Operational
RiskType: Current
BusinessImpact: Legal consequences, compromised historical access tracking
RiskDescription: Failure to retain access logs for the required period may result in regulatory penalties
RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated data retention policies", "2": "Regularly audit access log ret
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2557:
RiskId: 201
ComplianceId: 207
RiskTitle: Inaccurate Access Tracking
Criticality: High
PossibleDamage: Data breaches, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, regulatory fines
RiskDescription: Failure to accurately track access events may lead to data breaches or compliance vi
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly update logging tools", "2": "Implement access event correlation mechan
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2558:
RiskId: 201
ComplianceId: 207
RiskTitle: Inaccurate Access Tracking
Criticality: High
PossibleDamage: Data breaches, compliance violations
Category: Operational
RiskType: Current
BusinessImpact: Loss of sensitive data, regulatory fines
RiskDescription: Failure to accurately track access events may lead to data breaches or compliance vi
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update logging tools", "2": "Implement access event correlation mechan
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2559:
RiskId: 202
ComplianceId: 208
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data breach resulting in loss of sensitive information

Category: IT
RiskType: Residual
BusinessImpact: Financial loss, Reputation damage
RiskDescription: Failure to conduct quarterly security testing may lead to undetected vulnerabilities, inc
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated testing tools", "2": "Conduct manual assessments in additio
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2560:
RiskId: 202
ComplianceId: 208
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data breach resulting in loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Financial loss, Reputation damage
RiskDescription: Failure to conduct quarterly security testing may lead to undetected vulnerabilities, inc
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated testing tools", "2": "Conduct manual assessments in additio
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel

CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2561:
RiskId: 203
ComplianceId: 209
RiskTitle: Post-Change Vulnerability Risk
Criticality: Medium
PossibleDamage: Exploitation of vulnerabilities post-network changes
Category: IT
RiskType: Residual
BusinessImpact: Network downtime, Data loss
RiskDescription: Failure to test security systems after network changes may leave vulnerabilities undet
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement change management process to trigger post-change testing", "2": "Co
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2562:
RiskId: 203
ComplianceId: 209
RiskTitle: Post-Change Vulnerability Risk
Criticality: Medium
PossibleDamage: Exploitation of vulnerabilities post-network changes
Category: IT
RiskType: Residual
BusinessImpact: Network downtime, Data loss
RiskDescription: Failure to test security systems after network changes may leave vulnerabilities undet

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement change management process to trigger post-change testing", "2": "Co
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2563:
RiskId: 204
ComplianceId: 210
RiskTitle: Manual Assessment Gap Risk
Criticality: High
PossibleDamage: Missed vulnerabilities due to lack of manual assessments
Category: IT
RiskType: Residual
BusinessImpact: Data breach, Compliance violations
RiskDescription: Relying solely on automated tools may miss certain vulnerabilities that require manua
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Train IT security team on manual assessment techniques", "2": "Implement period
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2564:
RiskId: 204

ComplianceId: 210
RiskTitle: Manual Assessment Gap Risk
Criticality: High
PossibleDamage: Missed vulnerabilities due to lack of manual assessments
Category: IT
RiskType: Residual
BusinessImpact: Data breach, Compliance violations
RiskDescription: Relying solely on automated tools may miss certain vulnerabilities that require manua
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Train IT security team on manual assessment techniques", "2": "Implement period
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2565:
RiskId: 205
ComplianceId: 211
RiskTitle: Security Breach Due to Lack of Training
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Failure to provide annual security awareness training may lead to employees being u
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regularly scheduled training sessions", "2": "Tracking and monitoring training com
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2566:
RiskId: 205
ComplianceId: 211
RiskTitle: Security Breach Due to Lack of Training
Criticality: High
PossibleDamage: Financial losses, reputational damage, legal consequences
Category: Operational
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Failure to provide annual security awareness training may lead to employees being u
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly scheduled training sessions", "2": "Tracking and monitoring training com
CreatedAt: 2025-10-07 00:00:00
CreatedBy: vikram.patel
CreatedByName: Vikram Patel
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2567:
RiskId: 206
ComplianceId: 212
RiskTitle: Security Incident Due to Lack of New Employee Training
Criticality: Medium
PossibleDamage: Data breaches, compliance violations, reputational damage

Category: Operational
RiskType: Residual
BusinessImpact: Increased workload for HR and Security teams, potential legal consequences
RiskDescription: Failure to provide security training to new employees may result in them unknowingly
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Incorporate security training into onboarding process", "2": "Provide resources for
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2568:
RiskId: 207
ComplianceId: 213
RiskTitle: Inadequate Training Delivery
Criticality: Low
PossibleDamage: Security incidents due to lack of awareness, potential compliance violations
Category: Operational
RiskType: Residual
BusinessImpact: Loss of trust in HR and Security departments, potential legal consequences
RiskDescription: If HR and Security teams fail to effectively implement security awareness training, em
RiskLikelihood: 4
RiskImpact: 3
RiskExposureRating: 12
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Establish clear roles and responsibilities", "2": "Provide training for trainers", "3": "
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2569:
RiskId: 208
ComplianceId: 214
RiskTitle: Annual Policy Communication Risk
Criticality: Medium
PossibleDamage: Lack of awareness leading to policy violations and security breaches
Category: Operational
RiskType: Current
BusinessImpact: All business units handling cardholder data
RiskDescription: Failure to communicate the policy annually may result in personnel not being aware o
RiskLikelihood: 8
RiskImpact: 7
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Schedule regular policy communication sessions", "2": "Provide refresher training
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2570:
RiskId: 209
ComplianceId: 215
RiskTitle: Policy Update Communication Risk
Criticality: High
PossibleDamage: Outdated policy knowledge leading to non-compliance
Category: Operational
RiskType: Current
BusinessImpact: All business units handling cardholder data
RiskDescription: Failure to communicate policy updates may result in personnel following outdated pol

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a process for immediate policy update dissemination", "2": "Require ac
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2571:
RiskId: 210
ComplianceId: 216
RiskTitle: Policy Communication Responsibility Risk
Criticality: Medium
PossibleDamage: Lack of clear responsibility leading to communication gaps
Category: Operational
RiskType: Current
BusinessImpact: Security team
RiskDescription: Unclear responsibility for policy communication within the security team may result in
RiskLikelihood: 8
RiskImpact: 7
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Define clear roles and responsibilities within the security team", "2": "Provide train
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2572:
RiskId: 211

ComplianceId: 217
RiskTitle: Failure to Identify System Components
Criticality: High
PossibleDamage: Potential security breaches and non-compliance with PCI DSS standards
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties, legal consequences
RiskDescription: Failure to identify all system components within the CDE may lead to vulnerabilities a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular training for IT Security team on identifying system components", "2": "Imp
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2573:
RiskId: 212
ComplianceId: 218
RiskTitle: Inaccurate Scoping Process Documentation Retention
Criticality: High
PossibleDamage: Inaccurate scoping leading to potential data breaches or non-compliance fines
Category: Operational
RiskType: Current
BusinessImpact: All departments involved in PCI DSS compliance would be impacted by inaccurate sc
RiskDescription: Failure to retain documentation related to the scoping process may result in inaccurat
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular audits to ensure documentation retention compliance", "2": "Training for s
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2574:
RiskId: 213
ComplianceId: 219
RiskTitle: Compliance Officer Responsibility for Documentation Retention
Criticality: Medium
PossibleDamage: Documentation not being retained as required, leading to non-compliance
Category: Operational
RiskType: Current
BusinessImpact: Non-compliance with documentation retention requirements
RiskDescription: Failure to assign responsibility to the Compliance Officer for documentation retention
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Clearly define the Compliance Officer's responsibilities in the documentation reter
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2575:
RiskId: 214
ComplianceId: 220
RiskTitle: Unauthorized Access to Stored Documentation
Criticality: High
PossibleDamage: Unauthorized access or tampering of stored documentation

Category: IT
RiskType: Current
BusinessImpact: Compromised integrity of the scoping process
RiskDescription: Failure to securely store documentation related to the scoping process may lead to ur
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement access controls to restrict unauthorized access to documentation", "2"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2576:
RiskId: 215
ComplianceId: 221
RiskTitle: Unauthorized Access to CDE
Criticality: High
PossibleDamage: Data breaches, non-compliance penalties
Category: Operational
RiskType: Residual
BusinessImpact: Loss of sensitive data, financial penalties
RiskDescription: Unauthorized access to the CDE can result in data breaches and non-compliance per
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update firewall rules", "2": "Implement intrusion detection sy
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2577:
RiskId: 216
ComplianceId: 222
RiskTitle: Ineffective Segmentation
Criticality: Medium
PossibleDamage: Unauthorized access to the CDE
Category: Operational
RiskType: Residual
BusinessImpact: Risk of data breaches, non-compliance penalties
RiskDescription: Failure to review network segmentation annually may result in ineffective isolation of t
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Conduct regular penetration testing", "2": "Implement network monitoring tools", "3
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2578:
RiskId: 217
ComplianceId: 223
RiskTitle: Security Vulnerabilities in New Systems
Criticality: High
PossibleDamage: Unauthorized access to the CDE
Category: Operational
RiskType: Residual
BusinessImpact: Risk of data breaches, non-compliance penalties
RiskDescription: Failure to establish segmentation for new system deployments may introduce security

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Include segmentation in system deployment checklist", "2": "Conduct security ass
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2579:
RiskId: 218
ComplianceId: 224
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data
Category: IT
RiskType: Current
BusinessImpact: Data breach, loss of sensitive information
RiskDescription: Risk of unauthorized individuals gaining access to critical network segments and sens
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong access controls", "2": "Regularly review and update network se
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2580:
RiskId: 219

ComplianceId: 225
RiskTitle: Outdated Documentation Risk
Criticality: Medium
PossibleDamage: Misconfigurations due to outdated documentation
Category: IT
RiskType: Current
BusinessImpact: Network downtime, security vulnerabilities
RiskDescription: Risk of outdated documentation leading to misconfigurations in network segmentation
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated documentation update reminders", "2": "Regularly review a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2581:
RiskId: 220
ComplianceId: 226
RiskTitle: Documentation Accessibility Risk
Criticality: High
PossibleDamage: Delays in troubleshooting due to inaccessible documentation
Category: Operational
RiskType: Current
BusinessImpact: Operational inefficiencies, potential security incidents
RiskDescription: Risk of relevant personnel not being able to access critical network segmentation doc
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement role-based access controls for documentation repository", "2": "Regula
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2582:
RiskId: 221
ComplianceId: 230
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data exposure, financial penalties, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Legal and financial repercussions
RiskDescription: Risk of data breach due to third-party non-compliance with PCI DSS
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of third-party compliance", "2": "Data encryption measures", "3
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2583:
RiskId: 222
ComplianceId: 231
RiskTitle: Outdated Contract Risk
Criticality: Medium
PossibleDamage: Non-compliance, legal disputes, financial penalties

Category: Operational
RiskType: Current
BusinessImpact: Legal and financial repercussions
RiskDescription: Risk of non-compliance due to outdated contract terms with third-party service provide
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establishing contract review schedule", "2": "Automating contract renewal remind
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2584:
RiskId: 223
ComplianceId: 232
RiskTitle: Ambiguity in Service Scope Risk
Criticality: High
PossibleDamage: Misunderstandings, non-compliance, legal disputes
Category: Operational
RiskType: Current
BusinessImpact: Legal and financial repercussions
RiskDescription: Risk of misunderstandings and non-compliance due to unclear service scope and con
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Detailed contract drafting", "2": "Regular communication with service providers", "
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2585:
RiskId: 224
ComplianceId: 233
RiskTitle: Engagement of Non-Certified QSA
Criticality: High
PossibleDamage: Inaccurate assessments, potential data breaches, and regulatory fines
Category: Compliance
RiskType: Residual
BusinessImpact: Non-compliance penalties, reputational damage, financial losses
RiskDescription: Engaging a non-certified QSA may result in inaccurate assessments, potential data b
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify QSA certification status with the PCI Security Standards Council before en
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2586:
RiskId: 225
ComplianceId: 234
RiskTitle: Engagement of Inexperienced QSA
Criticality: Medium
PossibleDamage: Incomplete assessments, unidentified vulnerabilities, potential data breaches
Category: Compliance
RiskType: Residual
BusinessImpact: Non-compliance penalties, reputational damage, financial losses
RiskDescription: Engaging an inexperienced QSA may result in incomplete assessments, unidentified

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Request case studies or references from potential QSAs", "2": "Conduct interview
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2587:
RiskId: 226
ComplianceId: 235
RiskTitle: Engagement of Unreliable QSA
Criticality: High
PossibleDamage: Compromised assessments, potential data breaches, financial losses
Category: Compliance
RiskType: Residual
BusinessImpact: Non-compliance penalties, reputational damage, financial losses
RiskDescription: Neglecting reference checks may result in engaging unreliable QSAs with a history of
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Request and contact references provided by potential QSAs", "2": "Verify the auth
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2588:
RiskId: 227

ComplianceId: 236
RiskTitle: Delay in QSA Engagement
Criticality: High
PossibleDamage: Non-compliance with PCI DSS standards, potential fines
Category: Compliance
RiskType: Current
BusinessImpact: Non-compliance, financial penalties
RiskDescription: Failure to engage a QSA in a timely manner may result in non-compliance with PCI D
RiskLikelihood: 9
RiskImpact: 9
RiskExposureRating: 81
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear timeline for engagement process", "2": "Allocate dedicated resourc
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2589:
RiskId: 228
ComplianceId: 237
RiskTitle: Inadequate QSA Selection
Criticality: Medium
PossibleDamage: Incomplete assessment, non-compliance
Category: Compliance
RiskType: Current
BusinessImpact: Incomplete assessment, potential non-compliance
RiskDescription: Selecting an inadequate QSA may result in incomplete assessment of PCI DSS comp
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Establish clear evaluation criteria for QSAs", "2": "Conduct thorough due diligence
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2590:
RiskId: 229
ComplianceId: 238
RiskTitle: Mismatched QSA Selection
Criticality: Medium
PossibleDamage: Ineffective compliance assessment
Category: Compliance
RiskType: Current
BusinessImpact: Ineffective compliance assessment, potential cultural clashes
RiskDescription: Selecting a QSA that does not align with organizational values may result in ineffectiv
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop interview questions aligned with organizational values", "2": "Include key
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2591:
RiskId: 230
ComplianceId: 239
RiskTitle: Inadequate Vulnerability Scanning
Criticality: High
PossibleDamage: Potential data breaches and security incidents

Category: Operational
RiskType: Current
BusinessImpact: IT Security, Compliance
RiskDescription: Failure to verify ASV qualification may result in the ASV not meeting necessary stand
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Verify ASV qualification status with the PCI Security Standards Council", "2": "Ma
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2592:
RiskId: 231
ComplianceId: 240
RiskTitle: Disruptive Scanning Practices
Criticality: Medium
PossibleDamage: System downtime, data loss, service interruptions
Category: Operational
RiskType: Current
BusinessImpact: IT Security, Compliance
RiskDescription: Failure to ensure ASV capability for non-disruptive scans may result in disruptive scar
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Request demonstration of non-disruptive scanning capabilities from ASV", "2": "In
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2593:
RiskId: 232
ComplianceId: 241
RiskTitle: Incomplete Compliance Reporting
Criticality: High
PossibleDamage: Regulatory non-compliance and penalties
Category: Compliance
RiskType: Current
BusinessImpact: IT Security, Compliance
RiskDescription: Lack of agreement on compliance reporting with the ASV may result in incomplete or
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear compliance reporting requirements with ASV", "2": "Include compli
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2594:
RiskId: 233
ComplianceId: 242
RiskTitle: Undetected Vulnerabilities Due to Lack of ASV Engagement
Criticality: High
PossibleDamage: Undetected vulnerabilities may lead to data breaches and non-compliance penalties
Category: Operational
RiskType: Inherent
BusinessImpact: Potential financial losses, reputational damage, and legal consequences
RiskDescription: Failure to engage an ASV may result in vulnerabilities going undetected, increasing th

RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update the ASV contract to ensure it aligns with current requ
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2595:
RiskId: 234
ComplianceId: 243
RiskTitle: Miscommunication and Ineffective Management by IT Security Manager
Criticality: Medium
PossibleDamage: Miscommunication and ineffective management may lead to misunderstandings, del
Category: Operational
RiskType: Inherent
BusinessImpact: Operational inefficiencies, compliance violations, and potential financial losses
RiskDescription: Lack of clear communication and effective management by the IT Security Manager n
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide regular training and updates to the IT Security Manager on ASV engagem
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2596:
RiskId: 235

ComplianceId: 244
RiskTitle: Missed Vulnerability Scans Due to Delayed ASV Engagement
Criticality: Medium
PossibleDamage: Delayed engagement may result in missed vulnerability scans, leaving systems expo
Category: Operational
RiskType: Inherent
BusinessImpact: Increased vulnerability to cyber threats, potential data breaches, and compliance viola
RiskDescription: Delayed engagement of the ASV may result in missed vulnerability scans, leaving sys
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish automated reminders for ASV engagement deadlines", "2": "Implement
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2597:
RiskId: 236
ComplianceId: 245
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage.
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines, legal actions.
RiskDescription: Unauthorized access to cardholder data can lead to data breaches and financial losse
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement access controls and encryption", "2": "Regularly monitor data access l
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2598:
RiskId: 237
ComplianceId: 246
RiskTitle: Incomplete Compliance Assessment
Criticality: Medium
PossibleDamage: Non-compliance penalties, reputational damage, legal actions.
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, regulatory fines, loss of business opportunities.
RiskDescription: Failure to map data locations accurately may lead to incomplete compliance assessm
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated data discovery tools", "2": "Conduct regular data mapping e
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2599:
RiskId: 238
ComplianceId: 247
RiskTitle: Third-Party Non-Compliance
Criticality: High
PossibleDamage: Data breaches, regulatory fines, loss of customer trust.

Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal actions, reputational damage.
RiskDescription: Non-compliance by third parties with data security standards may lead to data breach
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular third-party audits", "2": "Include data location verification in vendo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2600:
RiskId: 239
ComplianceId: 248
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal consequences
RiskDescription: Unauthorized access to cardholder data due to ineffective network segmentation cont
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review and update of segmentation controls", "2": "Continuous monitoring
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2601:
RiskId: 240
ComplianceId: 249
RiskTitle: Outdated Segmentation Controls
Criticality: Medium
PossibleDamage: Increased risk of unauthorized access, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal consequences
RiskDescription: Failure to review and update segmentation controls annually may lead to outdated co
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly scheduled annual reviews of segmentation controls", "2": "Documentati
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2602:
RiskId: 241
ComplianceId: 250
RiskTitle: Lack of Documentation in Segmentation Design
Criticality: Medium
PossibleDamage: Difficulty in troubleshooting, lack of accountability
Category: Operational
RiskType: Residual
BusinessImpact: Operational inefficiencies, compliance challenges
RiskDescription: Inadequate documentation of segmentation design may lead to difficulties in troublesh

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Comprehensive documentation of segmentation design and implementation", "2":
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2603:
RiskId: 242
ComplianceId: 251
RiskTitle: Data Breach Risk from Non-Compliant Third-Party Providers
Criticality: High
PossibleDamage: Data breaches, financial penalties
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial losses
RiskDescription: Failure to ensure third-party compliance could result in data breaches and financial pe
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update contracts", "2": "Conduct regular assessments of thi
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2604:
RiskId: 243

ComplianceId: 252
RiskTitle: Misunderstandings Due to Outdated Contracts
Criticality: Medium
PossibleDamage: Misunderstandings, non-compliance
Category: Operational
RiskType: Residual
BusinessImpact: Disputes, non-compliance
RiskDescription: Failure to review and update contracts could lead to misunderstandings and disputes
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a contract review schedule", "2": "Update contracts promptly upon chan
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2605:
RiskId: 244
ComplianceId: 253
RiskTitle: Undetected Non-Compliance Risks
Criticality: High
PossibleDamage: Undetected non-compliance, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, financial penalties
RiskDescription: Failure to conduct regular assessments could result in undetected non-compliance ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish assessment schedule", "2": "Document assessment findings and remed
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2606:
RiskId: 245
ComplianceId: 254
RiskTitle: Incorrect SAQ Type Selection
Criticality: Medium
PossibleDamage: Non-compliance with PCI DSS requirements
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, reputational damage
RiskDescription: Selecting the wrong SAQ type can result in inadequate security measures being imple
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear SAQ selection criteria", "2": "Implement regular reviews of SAQ ty
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2607:
RiskId: 246
ComplianceId: 255
RiskTitle: Missed SAQ Completion Deadline
Criticality: High
PossibleDamage: Non-compliance with PCI DSS requirements

Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, reputational damage
RiskDescription: Failure to complete the SAQ annually can result in outdated security measures, expos
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate SAQ completion reminders", "2": "Implement escalation procedures for
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2608:
RiskId: 247
ComplianceId: 256
RiskTitle: Delayed SAQ Submission
Criticality: Medium
PossibleDamage: Non-compliance with PCI DSS requirements
Category: Operational
RiskType: Inherent
BusinessImpact: Financial losses, reputational damage
RiskDescription: Submitting the SAQ after the deadline can result in penalties and non-compliance witl
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate submission reminders", "2": "Establish escalation procedures for delaye
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2609:
RiskId: 248
ComplianceId: 257
RiskTitle: Non-Compliance with SAQ Remediation Documentation
Criticality: High
PossibleDamage: Potential fines, penalties, and reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Financial penalties, loss of reputation
RiskDescription: Failure to document remediation actions for non-compliant SAQ responses could resu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear documentation procedures", "2": "Implement regular training on SA
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2610:
RiskId: 249
ComplianceId: 258
RiskTitle: Late Submission of SAQ
Criticality: High
PossibleDamage: Fines, penalties, or suspension of payment processing services
Category: Compliance
RiskType: Current
BusinessImpact: Finance, Compliance
RiskDescription: Late submission of SAQs may result in compliance violations and financial penalties.

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear submission deadlines", "2": "Implement automated reminders for s
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2611:
RiskId: 250
ComplianceId: 259
RiskTitle: Incomplete SAQ Submission
Criticality: Medium
PossibleDamage: Compliance violations
Category: Compliance
RiskType: Current
BusinessImpact: Compliance, IT
RiskDescription: Incomplete SAQ submissions may result in non-compliance with PCI DSS requiremer
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide clear instructions on template usage", "2": "Implement review process for
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2612:
RiskId: 251

ComplianceId: 260
RiskTitle: Data Breach via Unauthorized Portal
Criticality: High
PossibleDamage: Data compromise, compliance violations
Category: IT
RiskType: Current
BusinessImpact: Finance, IT
RiskDescription: Submission of SAQs through unauthorized portals may result in data breaches and no
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls to portal", "2": "Regularly review portal access lo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2613:
RiskId: 252
ComplianceId: 261
RiskTitle: Late submission of RoC
Criticality: High
PossibleDamage: Fines, penalties, regulatory sanctions
Category: Compliance
RiskType: Current
BusinessImpact: Financial loss, reputational damage
RiskDescription: Failure to submit RoC within the required timeframe may result in regulatory consequ
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Establish clear submission timelines and responsibilities", "2": "Implement automa

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: Retail Banking

Item 2614:

RiskId: 253

ComplianceId: 262

RiskTitle: Inaccurate documentation of assessment findings

Criticality: Medium

PossibleDamage: Misinterpretation of assessment results, ineffective compliance measures

Category: Operational

RiskType: Current

BusinessImpact: Inefficient remediation efforts, compliance gaps

RiskDescription: Failure to accurately document assessment findings may lead to incorrect remediatio

RiskLikelihood: 7

RiskImpact: 6

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement documentation training programs", "2": "Conduct regular audits of asse

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 2615:

RiskId: 254

ComplianceId: 263

RiskTitle: Non-compliance with RoC template usage

Criticality: Low

PossibleDamage: Audit findings, inconsistencies in reporting

Category: Compliance
RiskType: Current
BusinessImpact: Resource wastage, compliance discrepancies
RiskDescription: Failure to use the RoC template for submission may result in audit findings and incons
RiskLikelihood: 5
RiskImpact: 3
RiskExposureRating: 15
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Provide template training sessions", "2": "Implement template usage checks befo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2616:
RiskId: 255
ComplianceId: 264
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Financial loss, reputational damage, legal consequences
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust
RiskDescription: Failure to conduct quarterly scans may result in undetected vulnerabilities leading to d
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training for IT Security Team on conducting scans", "2": "Imple
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division
Item 2617:
RiskId: 256
ComplianceId: 265
RiskTitle: Compliance Reporting Risk
Criticality: Medium
PossibleDamage: Regulatory fines, audit failures, reputational damage
Category: Compliance
RiskType: Residual
BusinessImpact: Negative audit outcomes, loss of compliance certifications
RiskDescription: Failure to report quarterly scan results may lead to non-compliance with regulatory re
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear reporting procedures and timelines", "2": "Implement secure data t
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2618:
RiskId: 257
ComplianceId: 266
RiskTitle: Submission Timeline Risk
Criticality: Medium
PossibleDamage: Prolonged exposure to security risks, potential data breaches
Category: Operational
RiskType: Residual
BusinessImpact: Increased vulnerability exposure, potential data loss
RiskDescription: Delayed submission of quarterly scan reports may result in unaddressed vulnerabilitie

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish automated reporting mechanisms for timely submissions", "2": "Impleme
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2619:
RiskId: 258
ComplianceId: 267
RiskTitle: Unauthorized Access to Payment Card Data
Criticality: High
PossibleDamage: Financial losses and reputational damage
Category: IT
RiskType: Residual
BusinessImpact: IT Security Team
RiskDescription: Unauthorized individuals gaining access to payment card data due to ineffective secu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enhanced access controls", "2": "Regular security training for employees", "3": "E
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2620:
RiskId: 259

ComplianceId: 268
RiskTitle: Data Breach Due to Delayed Response
Criticality: Medium
PossibleDamage: Loss of sensitive data and regulatory fines
Category: IT
RiskType: Residual
BusinessImpact: IT Security Team
RiskDescription: Sensitive payment card data being compromised due to delayed response to security
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Incident response drills", "2": "Automated incident response tools", "3": "Regular s
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2621:
RiskId: 260
ComplianceId: 269
RiskTitle: Security Gaps Due to Misinterpreted Results
Criticality: Medium
PossibleDamage: Increased vulnerability to cyber threats
Category: IT
RiskType: Residual
BusinessImpact: IT Security Team
RiskDescription: Misinterpretation of automated monitoring results leading to undetected security gaps
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 45
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Regular tool training sessions", "2": "Cross-verification of results", "3": "Enhanced
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2622:
RiskId: 261
ComplianceId: 270
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Potential data breaches and financial losses
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Unauthorized access to cardholder data can result in data breaches, financial losses,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls", "2": "Encrypt sensitive data at rest and in transi
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2623:
RiskId: 262
ComplianceId: 271
RiskTitle: Overlooking Critical PCI DSS Compliance Issues
Criticality: Medium
PossibleDamage: Non-compliance penalties and potential data breaches

Category: Operational
RiskType: Residual
BusinessImpact: Change Management Team
RiskDescription: Failure to review changes may result in overlooking critical PCI DSS compliance issue
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated change impact assessment tools", "2": "Conduct regular au
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2624:
RiskId: 263
ComplianceId: 272
RiskTitle: Uncontrolled System Changes
Criticality: High
PossibleDamage: Potential non-compliance penalties and data breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Lack of a formal change request process may result in uncontrolled system changes,
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish clear change request guidelines and approval workflows", "2": "Automat
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2625:
RiskId: 264
ComplianceId: 273
RiskTitle: Data Breach Due to Non-Compliance
Criticality: High
PossibleDamage: Loss of customer trust, financial penalties
Category: IT
RiskType: Residual
BusinessImpact: Finance, Compliance
RiskDescription: Failure to comply with PCI DSS requirements could lead to unauthorized access to pa
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular training on PCI DSS requirements", "2": "Implement multi-facto
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2626:
RiskId: 265
ComplianceId: 274
RiskTitle: Misinterpretation of Compliance Findings
Criticality: Medium
PossibleDamage: Incorrect actions taken based on misunderstood compliance status
Category: Operational
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Lack of clear communication of compliance findings could lead to stakeholders misun

RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish regular communication channels for compliance updates", "2": "Provide
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2627:
RiskId: 266
ComplianceId: 275
RiskTitle: Incomplete Compliance Documentation
Criticality: High
PossibleDamage: Audit failures, compliance gaps
Category: Compliance
RiskType: Residual
BusinessImpact: Compliance
RiskDescription: Failure to document compliance reviews and findings could result in audit failures and
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement a centralized compliance documentation system", "2": "Regularly revie
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2628:
RiskId: 267

ComplianceId: 276
RiskTitle: Unauthorized Access Due to Poor Documentation
Criticality: High
PossibleDamage: Unauthorized access to cardholder data, data breaches, financial losses.
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties, legal consequences.
RiskDescription: Failure to document firewall and router configurations may result in unauthorized acce
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated documentation tools", "2": "Regularly review and update do
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2629:
RiskId: 268
ComplianceId: 277
RiskTitle: Security Vulnerabilities from Untested Configurations
Criticality: Medium
PossibleDamage: Security breaches, network downtime, loss of data integrity.
Category: IT
RiskType: Residual
BusinessImpact: Disruption of network services, financial losses, reputational damage.
RiskDescription: Failure to test firewall and router configurations may introduce security vulnerabilities,
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement automated testing tools", "2": "Establish testing protocols and procedu
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2630:
RiskId: 269
ComplianceId: 278
RiskTitle: Non-Compliance Due to Infrequent Reviews
Criticality: High
PossibleDamage: Non-compliance with security standards, increased vulnerability to cyber threats, dat
Category: IT
RiskType: Residual
BusinessImpact: Financial penalties, reputational damage, legal consequences.
RiskDescription: Infrequent reviews of firewall and router configurations may lead to non-compliance w
RiskLikelihood: 8
RiskImpact: 8
RiskExposureRating: 64
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish a regular review schedule", "2": "Automate configuration review process
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2631:
RiskId: 270
ComplianceId: 279
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information

Category: IT
RiskType: Residual
BusinessImpact: Data confidentiality compromised, financial losses
RiskDescription: Unauthorized access to network resources and data due to ineffective firewall rules
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular review of firewall rules", "2": "Continuous monitoring of network traffic", "3
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2632:
RiskId: 271
ComplianceId: 280
RiskTitle: Firewall Configuration Vulnerability
Criticality: Medium
PossibleDamage: Increased vulnerability to cyber attacks, unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Data integrity compromised, financial losses
RiskDescription: Ineffective firewall configurations leading to potential security breaches and unauthori
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automated firewall configuration audits", "2": "Periodic penetration testing", "3": "I
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking
Item 2633:
RiskId: 272
ComplianceId: 281
RiskTitle: Device Configuration Vulnerability
Criticality: High
PossibleDamage: Unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Data confidentiality compromised, financial losses
RiskDescription: Misconfigured network devices leading to potential security vulnerabilities and unauth
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automated configuration audits", "2": "Configuration change management proces
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2634:
RiskId: 273
ComplianceId: 282
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breach, financial losses
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, legal implications
RiskDescription: Unauthorized access to cardholder data due to lack of network segmentation

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement firewall rules to restrict access", "2": "Regularly review and update acc
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2635:
RiskId: 274
ComplianceId: 283
RiskTitle: Access Control Failure Risk
Criticality: Medium
PossibleDamage: Data breach, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, legal implications
RiskDescription: Failure to enforce access controls leading to unauthorized access to cardholder data
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement strong authentication mechanisms", "2": "Regularly audit access logs",
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2636:
RiskId: 275

ComplianceId: 284
RiskTitle: Network Segmentation Review Risk
Criticality: Low
PossibleDamage: Unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, legal implications
RiskDescription: Failure to regularly review network segmentation leading to potential security gaps
RiskLikelihood: 5
RiskImpact: 4
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Conduct quarterly network segmentation audits", "2": "Implement automated mon
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2637:
RiskId: 276
ComplianceId: 285
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Data breaches and financial losses
Category: IT
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Unauthorized access through devices without personal firewall software could lead to
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Regular monitoring of firewall logs for suspicious activities", "2": "Periodic firewall
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2638:
RiskId: 277
ComplianceId: 286
RiskTitle: Ineffective Firewall Protection Risk
Criticality: Medium
PossibleDamage: Unauthorized access and data breaches
Category: IT
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Usage of unapproved firewall software could lead to ineffective protection, allowing ur
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular review of approved firewall software list to include latest security features
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2639:
RiskId: 278
ComplianceId: 287
RiskTitle: Misconfigured Firewall Settings Risk
Criticality: High
PossibleDamage: Vulnerabilities and unauthorized access

Category: IT
RiskType: Residual
BusinessImpact: All business units
RiskDescription: Misconfigured firewall settings could introduce vulnerabilities and allow unauthorized a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular audits of firewall configurations for compliance with security standards", "
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2640:
RiskId: 279
ComplianceId: 288
RiskTitle: Outdated Policy Risks
Criticality: High
PossibleDamage: Increased vulnerability to security breaches and non-compliance issues
Category: Operational
RiskType: Residual
BusinessImpact: IT, Compliance
RiskDescription: Failure to update policies regularly may result in staff following outdated procedures, l
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated reminders for policy updates", "2": "Conduct regular training
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2641:
RiskId: 280
ComplianceId: 289
RiskTitle: Training Gap Risks
Criticality: Medium
PossibleDamage: Lack of awareness leading to security incidents and non-compliance issues
Category: Operational
RiskType: Residual
BusinessImpact: IT, Compliance, Operations
RiskDescription: Failure to provide adequate training may result in staff not following security protocols
RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Develop interactive training modules", "2": "Conduct regular assessments to ensu
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2642:
RiskId: 281
ComplianceId: 290
RiskTitle: Policy Change Communication Risks
Criticality: Medium
PossibleDamage: Misinterpretation of new policies leading to non-compliance issues
Category: Operational
RiskType: Residual
BusinessImpact: IT, Compliance
RiskDescription: Failure to communicate policy changes promptly may result in staff not understanding

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish a clear communication protocol for policy updates", "2": "Provide trainin
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2643:
RiskId: 282
ComplianceId: 291
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Data breaches resulting in financial losses, reputational damage, and legal consequ
Category: Operational
RiskType: Residual
BusinessImpact: Significant impact on data security, compliance, and reputation
RiskDescription: Unauthorized access to retained cardholder data due to inadequate data retention co
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls", "2": "Encrypt sensitive data at rest and in transi
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2644:
RiskId: 283

ComplianceId: 292
RiskTitle: Data Storage Risk
Criticality: Medium
PossibleDamage: Increased storage costs, data security vulnerabilities, and regulatory non-compliance
Category: IT
RiskType: Residual
BusinessImpact: Impact on data storage efficiency, security, and compliance
RiskDescription: Accumulation of unnecessary cardholder data due to lack of clear data retention polic
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement data classification and retention tags", "2": "Regularly review and upda
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2645:
RiskId: 284
ComplianceId: 293
RiskTitle: Data Purging Risk
Criticality: High
PossibleDamage: Data breaches, regulatory fines, and reputational damage due to retained outdated
Category: Operational
RiskType: Residual
BusinessImpact: Significant impact on data security, compliance, and reputation
RiskDescription: Failure to timely purge outdated cardholder data leading to increased security risks ar
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement automated data purging tools", "2": "Establish data retention policies w
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2646:
RiskId: 285
ComplianceId: 294
RiskTitle: Weak Encryption Algorithm Vulnerability
Criticality: High
PossibleDamage: Potential unauthorized access to sensitive cardholder data
Category: IT
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties
RiskDescription: Failure to implement strong encryption algorithms may lead to data breaches and non
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption algorithms and key management practices", "2": "Imp
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2647:
RiskId: 286
ComplianceId: 295
RiskTitle: Weak Key Management Vulnerability
Criticality: Medium
PossibleDamage: Compromise of encryption keys and unauthorized access to cardholder data

Category: IT
RiskType: Residual
BusinessImpact: Data breaches, regulatory fines
RiskDescription: Inadequate key management practices may result in unauthorized access to sensitive
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement encryption key rotation policy", "2": "Use hardware security modules fo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2648:
RiskId: 287
ComplianceId: 296
RiskTitle: Data Transmission Encryption Vulnerability
Criticality: High
PossibleDamage: Interception of cardholder data during transmission
Category: IT
RiskType: Residual
BusinessImpact: Data exposure, loss of customer trust
RiskDescription: Failure to encrypt data during transmission may expose sensitive information to unaut
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement secure communication protocols (e.g., TLS)", "2": "Encrypt data at rest
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2649:
RiskId: 288
ComplianceId: 297
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Unauthorized access to sensitive data
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, financial penalties
RiskDescription: Failure to update key management procedures annually could result in unauthorized a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly scheduled annual reviews", "2": "Implementing access controls and log
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2650:
RiskId: 289
ComplianceId: 298
RiskTitle: Unauthorized Access Risk
Criticality: Medium
PossibleDamage: Data breaches and compromised encryption keys
Category: IT
RiskType: Residual
BusinessImpact: Loss of data confidentiality, regulatory fines
RiskDescription: Lack of proper access controls for key management activities could result in unauthor

RiskLikelihood: 5
RiskImpact: 7
RiskExposureRating: 35
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Role-based access control implementation", "2": "Regular monitoring of access lo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2651:
RiskId: 290
ComplianceId: 299
RiskTitle: Security Vulnerability Risk
Criticality: Low
PossibleDamage: Exposure to security threats
Category: Operational
RiskType: Residual
BusinessImpact: Data breaches, compromised encryption keys
RiskDescription: Insufficient training on key management best practices for IT security personnel could
RiskLikelihood: 3
RiskImpact: 4
RiskExposureRating: 12
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Regular training sessions on key management best practices", "2": "Certification p
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2652:
RiskId: 291

ComplianceId: 300
RiskTitle: Malware Infection Risk
Criticality: High
PossibleDamage: Data breaches, loss of sensitive information
Category: IT
RiskType: Residual
BusinessImpact: IT Security Team, Data Protection Team
RiskDescription: Failure to deploy and update anti-virus software may result in malware infections com
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update anti-virus software", "2": "Implement network segmentation to is
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2653:
RiskId: 292
ComplianceId: 301
RiskTitle: Outdated Anti-Virus Software Risk
Criticality: Medium
PossibleDamage: Inadequate protection against new malware threats
Category: IT
RiskType: Residual
BusinessImpact: IT Security Team, Data Protection Team
RiskDescription: Failure to update anti-virus software regularly may leave systems vulnerable to new m
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Schedule regular updates at non-peak hours", "2": "Implement automated update

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 2654:

RiskId: 293

ComplianceId: 302

RiskTitle: Anti-Virus Software Disabling Risk

Criticality: High

PossibleDamage: Exposure to malware attacks

Category: IT

RiskType: Residual

BusinessImpact: IT Security Team, Data Protection Team

RiskDescription: Unauthorized disabling of anti-virus software may compromise system security and ex

RiskLikelihood: 7

RiskImpact: 9

RiskExposureRating: 63

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement user access controls", "2": "Monitor software disablement attempts", "3

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 2655:

RiskId: 294

ComplianceId: 303

RiskTitle: Data Breach Due to Unpatched Vulnerabilities

Criticality: High

PossibleDamage: Data breach leading to financial losses, reputational damage, and regulatory penalti

Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust, legal consequences.
RiskDescription: Failure to deploy critical security patches may expose systems to known vulnerabilitie
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate patch deployment processes", "2": "Regularly monitor patch status and
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2656:
RiskId: 295
ComplianceId: 304
RiskTitle: Cyber Attack Exploiting Unpatched Vulnerabilities
Criticality: Medium
PossibleDamage: Data loss, system compromise, reputational damage.
Category: IT
RiskType: Residual
BusinessImpact: Disruption of operations, loss of customer trust, legal consequences.
RiskDescription: Failure to prioritize patch deployment based on risk assessments may expose critical
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish risk assessment criteria for patch prioritization", "2": "Regularly review a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2657:
RiskId: 296
ComplianceId: 305
RiskTitle: Compliance Violations Due to Inadequate Patch Tracking
Criticality: Medium
PossibleDamage: Penalties, legal consequences, reputational damage.
Category: IT
RiskType: Residual
BusinessImpact: Financial losses, loss of customer trust, regulatory scrutiny.
RiskDescription: Lack of visibility into patch status may lead to non-compliance with security policies a
RiskLikelihood: 7
RiskImpact: 7
RiskExposureRating: 49
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated patch status monitoring", "2": "Regularly audit patch manag
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2658:
RiskId: 297
ComplianceId: 306
RiskTitle: Insecure Code Vulnerabilities
Criticality: High
PossibleDamage: Data breaches, unauthorized access, compromised systems
Category: IT
RiskType: Current
BusinessImpact: Disruption of business operations, loss of sensitive data
RiskDescription: Failure to implement secure coding practices can lead to exploitable vulnerabilities in

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular code reviews", "2": "Security testing at each phase of development", "3":
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2659:
RiskId: 298
ComplianceId: 307
RiskTitle: Undetected Vulnerabilities
Criticality: Medium
PossibleDamage: Security breaches, data leaks, compromised systems
Category: IT
RiskType: Current
BusinessImpact: Loss of customer trust, financial losses
RiskDescription: Failure to conduct security assessments can result in undetected vulnerabilities that c
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular security assessments", "2": "Penetration testing", "3": "Continuous monito
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2660:
RiskId: 299

ComplianceId: 308
RiskTitle: Weak Security Controls
Criticality: High
PossibleDamage: Data breaches, cyber attacks, regulatory fines
Category: IT
RiskType: Current
BusinessImpact: Financial losses, reputational damage
RiskDescription: Failure to integrate security practices can lead to weaknesses in security controls and
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Security training", "2": "Regular security audits", "3": "Incident response planning"
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2661:
RiskId: 300
ComplianceId: 309
RiskTitle: Unauthorized Access Risk
Criticality: High
PossibleDamage: Unauthorized access to cardholder data, potential data breaches
Category: Operational
RiskType: Residual
BusinessImpact: IT Security, Compliance
RiskDescription: Risk of unauthorized users gaining access to sensitive cardholder data, leading to pot
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: {"1": "Implement strong access controls", "2": "Regularly review user access permissior

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Compliance Division

Item 2662:

RiskId: 301

ComplianceId: 310

RiskTitle: Multi-Factor Authentication Risk

Criticality: Medium

PossibleDamage: Unauthorized access, data breaches

Category: Operational

RiskType: Residual

BusinessImpact: IT Security

RiskDescription: Risk of unauthorized users gaining access to sensitive cardholder data due to lack of

RiskLikelihood: 6

RiskImpact: 7

RiskExposureRating: 42

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: {"1": "Implement multi-factor authentication solutions", "2": "Regularly review and updat

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Retail Banking

Item 2663:

RiskId: 302

ComplianceId: 311

RiskTitle: Annual Authentication Review Risk

Criticality: Low

PossibleDamage: Outdated or insecure authentication methods, increased risk of unauthorized access

Category: Operational
RiskType: Residual
BusinessImpact: IT Security
RiskDescription: Risk of using outdated or insecure authentication methods due to lack of annual revie
RiskLikelihood: 4
RiskImpact: 3
RiskExposureRating: 12
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Establish regular review schedules", "2": "Implement automated authentication m
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2664:
RiskId: 303
ComplianceId: 312
RiskTitle: Unauthorized Access to Cardholder Data Storage Areas
Criticality: High
PossibleDamage: Data breaches, compliance violations, financial losses.
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal consequences, financial penalties.
RiskDescription: Unauthorized individuals gaining access to areas storing cardholder data, leading to p
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement biometric access controls", "2": "Regularly audit access logs", "3": "Imp
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2665:
RiskId: 304
ComplianceId: 313
RiskTitle: Unauthorized Access by Posing as Employees
Criticality: Medium
PossibleDamage: Data breaches, compliance violations, reputational damage.
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal consequences, reputational damage.
RiskDescription: Unauthorized individuals posing as employees gaining access to sensitive areas stori
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement ID badge verification checkpoints", "2": "Regularly audit ID badge issu
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2666:
RiskId: 305
ComplianceId: 314
RiskTitle: Former Employees Retaining Access Post-Termination
Criticality: High
PossibleDamage: Data breaches, compliance violations, financial losses.
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal consequences, financial penalties.
RiskDescription: Former employees retaining access to sensitive areas storing cardholder data post-te

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automate access revocation process upon termination", "2": "Regularly review ac
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2667:
RiskId: 306
ComplianceId: 315
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: Unauthorized access to cardholder data can lead to data breaches, financial losses, a
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strong authentication mechanisms", "2": "Regularly review and update
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking

Item 2668:
RiskId: 307

ComplianceId: 316
RiskTitle: Miscommunication of Access Control Policies
Criticality: Medium
PossibleDamage: Misunderstandings, non-compliance, increased risk of unauthorized access
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: Miscommunication of access control policies can lead to misunderstandings, non-com
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear communication channels for policy updates", "2": "Conduct regula
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2669:
RiskId: 308
ComplianceId: 317
RiskTitle: Outdated Access Control Policies
Criticality: High
PossibleDamage: Increased risk of unauthorized access, data breaches
Category: Operational
RiskType: Residual
BusinessImpact: All business units handling cardholder data
RiskDescription: Failure to review access control policies annually may lead to outdated controls, incre
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Establish clear review timelines for policies", "2": "Conduct regular audits to asses
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2670:
RiskId: 309
ComplianceId: 318
RiskTitle: Data Breach Due to Unauthorized Access
Criticality: High
PossibleDamage: Loss of sensitive data, financial penalties, reputational damage
Category: Operational
RiskType: Current
BusinessImpact: Financial loss, damage to reputation, legal consequences
RiskDescription: Unauthorized access to critical system components can lead to data breaches and co
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls and user authentication measures", "2": "Regula
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2671:
RiskId: 310
ComplianceId: 319
RiskTitle: Delayed Detection of Security Breaches
Criticality: Medium
PossibleDamage: Extended exposure to security threats, data loss, compliance violations

Category: Operational
RiskType: Current
BusinessImpact: Financial loss, damage to reputation, legal consequences
RiskDescription: Failure to review audit trails daily may result in delayed detection of security breaches
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate alerts for suspicious activities in audit logs", "2": "Establish incident resp
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2672:
RiskId: 311
ComplianceId: 320
RiskTitle: Unauthorized Modification of Audit Logs
Criticality: High
PossibleDamage: Concealment of security incidents, non-compliance, legal consequences
Category: Operational
RiskType: Current
BusinessImpact: Financial loss, damage to reputation, legal consequences
RiskDescription: Unauthorized tampering or deletion of audit logs can lead to the concealment of secu
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement strict access controls for audit logs", "2": "Encrypt audit logs to prevent
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2673:
RiskId: 312
ComplianceId: 321
RiskTitle: Unidentified Vulnerabilities in Network
Criticality: High
PossibleDamage: Increased risk of unauthorized access or data breaches
Category: IT
RiskType: Current
BusinessImpact: Potential data breaches, financial losses, reputational damage
RiskDescription: Failure to conduct quarterly internal vulnerability scans may result in unidentified vuln
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement patches and updates promptly", "2": "Implement network segmentation
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Retail Banking
Item 2674:
RiskId: 313
ComplianceId: 322
RiskTitle: Failure to Conduct Annual Penetration Testing
Criticality: High
PossibleDamage: Potential data breaches, financial losses, reputational damage
Category: IT
RiskType: Current
BusinessImpact: Potential data breaches, financial losses, reputational damage
RiskDescription: Failure to conduct annual penetration testing may result in unidentified vulnerabilities

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement recommendations from penetration testing", "2": "Regularly update sec
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2675:
RiskId: 314
ComplianceId: 323
RiskTitle: Unidentified Vulnerabilities in External Network
Criticality: High
PossibleDamage: Increased risk of unauthorized access or data breaches
Category: IT
RiskType: Current
BusinessImpact: Potential data breaches, financial losses, reputational damage
RiskDescription: Failure to conduct quarterly external vulnerability scans may result in unidentified vuln
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement patches and updates promptly", "2": "Implement network segmentation
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2676:
RiskId: 315

ComplianceId: 327
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Financial losses and reputational damage
Category: IT
RiskType: Inherent
BusinessImpact: Loss of customer trust and regulatory fines
RiskDescription: Unauthorized access to cardholder data leading to data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement data loss prevention tools", "2": "Regularly conduct security awareness
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2677:
RiskId: 316
ComplianceId: 328
RiskTitle: New Vulnerabilities Risk
Criticality: Medium
PossibleDamage: Data leakage and unauthorized access
Category: IT
RiskType: Inherent
BusinessImpact: Loss of sensitive data and regulatory non-compliance
RiskDescription: Exposure to new vulnerabilities due to changes in the environment
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium
RiskMitigation: {"1": "Implement vulnerability scanning tools", "2": "Regularly update security configurat
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2678:
RiskId: 317
ComplianceId: 329
RiskTitle: Risk Documentation Loss
Criticality: Low
PossibleDamage: Ineffective risk management and lack of historical data
Category: IT
RiskType: Inherent
BusinessImpact: Inability to track risks and mitigation progress
RiskDescription: Loss of documented risk assessment findings leading to lack of visibility into risks and
RiskLikelihood: 4
RiskImpact: 3
RiskExposureRating: 12
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Implement version control for risk documents", "2": "Regularly backup risk docume
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2679:
RiskId: 318
ComplianceId: 330
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Financial loss, reputational damage

Category: Operational
RiskType: Current
BusinessImpact: Potential financial loss and damage to reputation
RiskDescription: Unauthorized access to cardholder data leading to data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for cardholder data", "2": "Regularly update security protoco
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit

Item 2680:
RiskId: 319
ComplianceId: 331
RiskTitle: Policy Non-Compliance Risk
Criticality: Medium
PossibleDamage: Penalties for non-compliance, increased vulnerability to security threats
Category: Operational
RiskType: Current
BusinessImpact: Potential penalties and increased security risks
RiskDescription: Misunderstanding or ignorance of updated security policies leading to non-compliance
RiskLikelihood: 7
RiskImpact: 6
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Provide detailed policy change notifications", "2": "Offer additional training resourc
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2681:
RiskId: 320
ComplianceId: 332
RiskTitle: Social Engineering Risk
Criticality: Low
PossibleDamage: Data breaches, unauthorized access
Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches and unauthorized access
RiskDescription: Decreased security awareness leading to susceptibility to social engineering attacks
RiskLikelihood: 5
RiskImpact: 4
RiskExposureRating: 20
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Low
RiskMitigation: {"1": "Provide regular security reminders", "2": "Conduct phishing simulation exercises",
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2682:
RiskId: 321
ComplianceId: 333
RiskTitle: Data Breach Incident
Criticality: High
PossibleDamage: Loss of sensitive cardholder data, financial penalties, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: IT, Legal, Compliance
RiskDescription: A security breach resulting in unauthorized access to cardholder data, leading to pote

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement encryption for cardholder data", "2": "Enhance network monitoring for e
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2683:
RiskId: 322
ComplianceId: 334
RiskTitle: Outdated Incident Response Plan
Criticality: Medium
PossibleDamage: Ineffective response to security breaches, increased risk of data loss
Category: Operational
RiskType: Residual
BusinessImpact: IT, Legal, Compliance
RiskDescription: An outdated incident response plan may not address current security threats effective
RiskLikelihood: 6
RiskImpact: 8
RiskExposureRating: 48
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regularly review and update the incident response plan", "2": "Conduct regular tra
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2684:
RiskId: 323

ComplianceId: 335
RiskTitle: Inadequate Incident Response Preparedness
Criticality: High
PossibleDamage: Inadequate preparedness for security breaches, delayed response times
Category: Operational
RiskType: Residual
BusinessImpact: IT, Legal, Compliance
RiskDescription: Inadequate preparedness for security breaches may result in delayed response times
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Conduct regular drills and simulations to test readiness", "2": "Implement lessons
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2685:
RiskId: 324
ComplianceId: 336
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Loss of customer trust, financial penalties, legal consequences
Category: IT
RiskType: Residual
BusinessImpact: Potential financial losses and reputational damage
RiskDescription: Failure to review compensating controls annually may result in undetected vulnerabili
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Conduct regular assessments as per schedule", "2": "Implement automated monit
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2686:
RiskId: 325
ComplianceId: 337
RiskTitle: Cyber Threat Vulnerability Risk
Criticality: Medium
PossibleDamage: Data breaches, unauthorized access, financial losses
Category: IT
RiskType: Residual
BusinessImpact: Increased risk of cyber attacks and potential data breaches
RiskDescription: Ineffective integration of compensating controls with existing security measures may c
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Conduct thorough integration testing before deployment", "2": "Regularly monitor
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2687:
RiskId: 326
ComplianceId: 338
RiskTitle: Outdated Controls Risk
Criticality: High
PossibleDamage: Increased vulnerability to cyber threats, potential data breaches

Category: IT
RiskType: Residual
BusinessImpact: Potential security breaches and financial losses
RiskDescription: Failure to re-evaluate compensating controls after significant changes may result in ou
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement change management process for control updates", "2": "Conduct imme
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2688:
RiskId: 327
ComplianceId: 339
RiskTitle: Non-Compliance with Documentation Requirements
Criticality: Medium
PossibleDamage: Increased security risks and potential fines for non-compliance
Category: Compliance
RiskType: Residual
BusinessImpact: Direct impact on IT and Compliance operations
RiskDescription: Failure to document compensating controls may result in audit failures and security vu
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Regular training on documentation procedures", "2": "Automated documentation t
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit
Item 2689:
RiskId: 328
ComplianceId: 340
RiskTitle: Ineffective Controls due to Outdated Documentation
Criticality: High
PossibleDamage: Increased security risks and potential breaches due to ineffective controls
Category: Compliance
RiskType: Residual
BusinessImpact: Direct impact on IT and Compliance operations
RiskDescription: Outdated documentation may lead to ineffective compensating controls and security v
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Automated documentation update reminders", "2": "Regular control environment a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2690:
RiskId: 329
ComplianceId: 341
RiskTitle: Unauthorized Access to Compensating Controls Documentation
Criticality: Medium
PossibleDamage: Compromised control effectiveness and potential security breaches
Category: Compliance
RiskType: Residual
BusinessImpact: Direct impact on IT and Compliance operations
RiskDescription: Unauthorized access to compensating controls documentation may compromise cont

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Encryption of stored documentation", "2": "Access control mechanisms implement
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2691:
RiskId: 330
ComplianceId: 342
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: IT
RiskType: Residual
BusinessImpact: Disruption of business operations, financial liabilities
RiskDescription: Unauthorized access to cardholder data due to inadequate firewall protection
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement multi-factor authentication", "2": "Encrypt sensitive data in transit and a
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2692:
RiskId: 331

ComplianceId: 343
RiskTitle: System Vulnerabilities Exploited
Criticality: High
PossibleDamage: Data breaches, financial losses
Category: IT
RiskType: Residual
BusinessImpact: Disruption of business operations, financial liabilities
RiskDescription: Exploitation of system vulnerabilities due to insecure configurations
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement regular patch management procedures", "2": "Enforce strong passwor
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit

Item 2693:
RiskId: 332
ComplianceId: 344
RiskTitle: Default Passwords Exploited
Criticality: High
PossibleDamage: Unauthorized access, data breaches
Category: IT
RiskType: Residual
BusinessImpact: Disruption of business operations, financial liabilities
RiskDescription: Exploitation of default vendor passwords leading to unauthorized access
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement password complexity requirements", "2": "Enforce regular password ch
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2694:
RiskId: 333
ComplianceId: 345
RiskTitle: Data Breach Due to Lack of Encryption
Criticality: High
PossibleDamage: Financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Unauthorized access to cardholder data during transmission leading to data breaches
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly update encryption protocols to meet industry standards", "2": "Impleme
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2695:
RiskId: 334
ComplianceId: 346
RiskTitle: Data Breach Due to Delayed Encryption Implementation
Criticality: Medium
PossibleDamage: Operational disruptions, financial losses

Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, regulatory fines
RiskDescription: Delayed encryption implementation leading to potential data breaches during network
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish clear timelines for encryption implementation during network deploymer
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2696:
RiskId: 335
ComplianceId: 347
RiskTitle: Data Vulnerabilities Due to Inadequate Encryption Implementation
Criticality: High
PossibleDamage: Data breaches, regulatory fines
Category: Operational
RiskType: Residual
BusinessImpact: Loss of customer trust, legal consequences
RiskDescription: Inadequate encryption implementation by network administrators leading to data vuln
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly assess network administrator compliance with encryption protocols", "2
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2697:
RiskId: 336
ComplianceId: 348
RiskTitle: Unauthorized Access to Cardholder Data
Criticality: High
PossibleDamage: Data breaches, financial losses, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal consequences, reputational damage
RiskDescription: Unauthorized access to cardholder data can lead to data breaches, financial losses, a
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regularly review and update access control policies", "2": "Implement multi-factor
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2698:
RiskId: 337
ComplianceId: 349
RiskTitle: Outdated Access Rights
Criticality: Medium
PossibleDamage: Unauthorized access, data breaches, financial losses
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal consequences
RiskDescription: Outdated access rights can lead to unauthorized access to cardholder data, resulting

RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 42
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Automate access rights review process", "2": "Implement access rights approval v
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking
Item 2699:
RiskId: 338
ComplianceId: 350
RiskTitle: Insufficient Access Logging
Criticality: High
PossibleDamage: Security incidents, compliance violations, reputational damage
Category: Operational
RiskType: Residual
BusinessImpact: Financial losses, legal consequences, reputational damage
RiskDescription: Lack of visibility into user access through access logs can lead to security incidents, c
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Enable detailed logging of access activities", "2": "Regularly review access logs fo
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: IT Operations Unit
Item 2700:
RiskId: 339

ComplianceId: 351
RiskTitle: Data Breach Risk
Criticality: High
PossibleDamage: Undetected vulnerabilities leading to potential data breaches
Category: IT
RiskType: Residual
BusinessImpact: Financial loss, reputational damage
RiskDescription: Failure to conduct quarterly testing may result in undetected vulnerabilities in security
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 72
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Implement automated testing tools", "2": "Conduct regular vulnerability assessme
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2701:
RiskId: 340
ComplianceId: 352
RiskTitle: Security Breach Risk
Criticality: High
PossibleDamage: Delayed detection of security breaches and unauthorized access
Category: IT
RiskType: Residual
BusinessImpact: Financial loss, reputational damage
RiskDescription: Lack of continuous monitoring may result in delayed detection of security breaches ar
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 76.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: High
RiskMitigation: {"1": "Implement real-time monitoring tools", "2": "Establish incident response procedure
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2702:
RiskId: 341
ComplianceId: 353
RiskTitle: Vulnerability Assessment Risk
Criticality: Medium
PossibleDamage: Missed critical vulnerabilities leading to security breaches
Category: IT
RiskType: Residual
BusinessImpact: Financial loss, reputational damage
RiskDescription: Manual vulnerability assessments may miss critical vulnerabilities, leading to potentia
RiskLikelihood: 7
RiskImpact: 7
RiskExposureRating: 52.5
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Implement automated vulnerability scanning tools", "2": "Regularly update vulnera
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking

Item 2703:
RiskId: 342
ComplianceId: 354
RiskTitle: Outdated Information Security Policy
Criticality: High
PossibleDamage: Increased vulnerability to security breaches

Category: Operational
RiskType: Current
BusinessImpact: Potential data breaches and loss of sensitive information
RiskDescription: Failure to update the information security policy annually may result in outdated secur
RiskLikelihood: 7
RiskImpact: 9
RiskExposureRating: 63
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Regular policy reviews and updates", "2": "Feedback solicitation from stakeholder
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2704:
RiskId: 343
ComplianceId: 355
RiskTitle: Lack of Stakeholder Feedback
Criticality: Medium
PossibleDamage: Policy misalignment with security needs
Category: Operational
RiskType: Current
BusinessImpact: Ineffective security measures
RiskDescription: Failure to collect feedback from stakeholders may result in policy misalignment with s
RiskLikelihood: 5
RiskImpact: 6
RiskExposureRating: 30
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: {"1": "Establish feedback collection mechanisms", "2": "Incorporate feedback into policy
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit
Item 2705:
RiskId: 344
ComplianceId: 356
RiskTitle: Infrequent Policy Reviews
Criticality: High
PossibleDamage: Increased security risks
Category: Operational
RiskType: Current
BusinessImpact: Potential security breaches
RiskDescription: Failure to review the information security policy as needed may result in an outdated p
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 56
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: {"1": "Establish criteria for additional reviews", "2": "Conduct reviews based on security
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division
Item 2706:
RiskId: 396
ComplianceId: None
RiskTitle: Unmonitored Admin Console Access from Public Network
Criticality: High
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust e
Category: Operational
RiskType: Current
BusinessImpact: High
RiskDescription: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to u

RiskLikelihood: 4
RiskImpact: 5
RiskExposureRating: 20
RiskMultiplierX: 0.5
RiskMultiplierY: 0.5
RiskPriority: Medium
RiskMitigation: Implement control hardening per standard, Enable continuous monitoring with a lerting
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2707:
RiskId: 397
ComplianceId: None
RiskTitle: Shadow IT File-Sharing Tools Cause Data Leakage
Criticality: Medium
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust e
Category: Technology Risk
RiskType: Current
BusinessImpact: None
RiskDescription: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to u
RiskLikelihood: 1
RiskImpact: 3
RiskExposureRating: 3
RiskMultiplierX: 0.5
RiskMultiplierY: 0.5
RiskPriority: Medium
RiskMitigation: Implement control hardening per standard, Enable continuous monitoring with a lerting
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2708:
RiskId: 398

ComplianceId: None
RiskTitle: Unauthorized API Access Due to Token Mismanagement
Criticality: High
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust e
Category: Operational
RiskType: Current
BusinessImpact: None
RiskDescription: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to u
RiskLikelihood: 1
RiskImpact: 7
RiskExposureRating: 7
RiskMultiplierX: 0.5
RiskMultiplierY: 0.5
RiskPriority: Medium
RiskMitigation: Implement control hardening per standard, Enable continuous monitoring with a lerting
CreatedAt: 2025-10-07 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2709:
RiskId: 399
ComplianceId: None
RiskTitle: Weak Vendor VPN Authentication Causes Lateral Movement Risk
Criticality: High
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust e
Category: Operational
RiskType: Current
BusinessImpact: None
RiskDescription: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to u
RiskLikelihood: 1
RiskImpact: 7
RiskExposureRating: 7
RiskMultiplierX: 0.5
RiskMultiplierY: 0.5

RiskPriority: Medium

RiskMitigation: Implement control hardening per standard, Enable continuous monitoring with a lerting

CreatedAt: 2025-10-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Customer Service

BusinessUnitName: Retail Banking

Item 2710:

RiskId: 391

ComplianceId: 1783

RiskTitle: Unauthorized access to sensitive data

Criticality: Medium

PossibleDamage: Heavy trading losses, fraud, system failures

Category: People Risk

RiskType: Residual

BusinessImpact: Operational Disruption

RiskDescription: sgrzjsrsjrsx

RiskLikelihood: 6

RiskImpact: 8

RiskExposureRating: 19.2

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: afefe■afefef

CreatedAt: 2025-10-04 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 2711:

RiskId: 365

ComplianceId: 1783

RiskTitle: Non-Compliance of Market & Operational Risk Capital Compliance

Criticality: High

PossibleDamage: Insufficient capital buffers to cover market and operational risks

Category: Process Risk
RiskType: Current
BusinessImpact: Revenue Loss, Customer Impact
RiskDescription: Capital adequacy for trading book exposures & operational failures
RiskLikelihood: 1
RiskImpact: 1
RiskExposureRating: 1
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: Conduct a thorough review of current capital adequacy ratios
CreatedAt: 2025-09-30 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2712:
RiskId: 385
ComplianceId: 1801
RiskTitle: Collateral Valuation & Dispute Resolution Risk
Criticality: Critical
PossibleDamage: Failure to properly value collateral and resolve margin disputes, leading to increased
Category: Operational
RiskType: Current
BusinessImpact: Failure to accurately value posted collateral, resulting in unmitigated counterparty exp
RiskDescription: Failure to resolve disputes over collateral values and margin calls, risking potential fin
RiskLikelihood: 9
RiskImpact: 10
RiskExposureRating: 0.92
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Ensure daily independent collateral valuation, improve dispute resolution processes for
CreatedAt: 2025-08-20 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2713:
RiskId: 384
ComplianceId: 1800
RiskTitle: Derivative Exposure Backtesting & Validation Risk
Criticality: High
PossibleDamage: Failure to backtest and validate derivative exposure models, leading to underreporte
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate backtesting of derivatives models, leading to underestimation of counterpa
RiskDescription: Failure to account for extreme market movements in derivative exposure models, risk
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 0.89
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: Improve derivative exposure backtesting processes, ensure model validation aligns witl
CreatedAt: 2025-08-19 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: IT Operations Unit

Item 2714:
RiskId: 383
ComplianceId: 1799
RiskTitle: Portfolio Stress Testing – Concentration Risk Incident
Criticality: Critical
PossibleDamage: Failure to address portfolio concentration risks during stress testing, leading to unmi
Category: Operational
RiskType: Current
BusinessImpact: Failure to perform stress testing on concentrated exposures, increasing risk of signific
RiskDescription: Missed or poorly simulated concentration risks leading to failure to maintain proper ca

RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 0.91
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Conduct targeted stress tests for concentrated portfolio risks, update models for better
CreatedAt: 2025-08-18 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2715:
RiskId: 382
ComplianceId: 1798
RiskTitle: Macroeconomic Stress Testing Supervisory Reporting Risk
Criticality: High
PossibleDamage: Failure to report macroeconomic stress test results to regulators on time, leading to
Category: Operational
RiskType: Current
BusinessImpact: Inability to meet regulatory reporting deadlines for stress test results, resulting in non-
RiskDescription: Failure to align stress test results with regulatory guidelines, risking supervisory penal
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 0.93
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Ensure timely reporting of stress test results, improve coordination with regulatory bodie
CreatedAt: 2025-08-17 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2716:
RiskId: 381

ComplianceId: 1797
RiskTitle: Pillar 3 Internal Validation & Audit Risk
Criticality: Critical
PossibleDamage: Failure to internally validate Pillar 3 disclosures, leading to incomplete or inaccurate
Category: Operational
RiskType: Current
BusinessImpact: Inaccurate or incomplete validation of Pillar 3 reports, potentially leading to regulatory
RiskDescription: Failure to validate risk-weighted assets and capital ratios, exposing the bank to poten
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 0.94
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Strengthen internal validation and audit procedures for Pillar 3 disclosures, enhance re
CreatedAt: 2025-08-16 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Compliance Division

Item 2717:
RiskId: 380
ComplianceId: 1796
RiskTitle: Leverage Ratio Stress Testing & Reporting Risk
Criticality: High
PossibleDamage: Failure to conduct appropriate stress tests for leverage ratios, leading to underrepor
Category: Operational
RiskType: Current
BusinessImpact: Failure to assess the impact of leverage ratio fluctuations, leading to unreported finan
RiskDescription: Inaccurate or incomplete leverage ratio stress testing, exposing the bank to capital sh
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 0.88
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: Review leverage ratio stress test scenarios, update reporting models for full Basel III co

CreatedAt: 2025-08-15 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 2718:

RiskId: 379

ComplianceId: 1795

RiskTitle: NSFR Compliance Risk

Criticality: Critical

PossibleDamage: Failure to meet the NSFR requirements, leading to long-term liquidity risk exposure.

Category: Operational

RiskType: Current

BusinessImpact: Failure to maintain sufficient stable funding over a one-year horizon, increasing liquid

RiskDescription: Inadequate stable funding sources and misalignment of funding with stable asset requ

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 9

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: Increase long-term funding sources, align funding strategies with stable asset requirem

CreatedAt: 2025-08-14 00:00:00

CreatedBy: radha.sharma

CreatedByName: Radha Sharma

DepartmentName: Risk Management

BusinessUnitName: Compliance Division

Item 2719:

RiskId: 378

ComplianceId: 1794

RiskTitle: LCR Stress Testing & Reporting Risk

Criticality: Critical

PossibleDamage: Failure to conduct appropriate LCR stress tests and timely reporting, risking non-cor

Category: Operational
RiskType: Current
BusinessImpact: Inability to meet short-term liquidity needs during a crisis, potentially resulting in finan
RiskDescription: Failure to properly report liquidity stress test results, exposing the bank to regulatory p
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 9
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Ensure monthly liquidity stress testing, improve LCR reporting accuracy, and meet regu
CreatedAt: 2025-08-13 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking

Item 2720:
RiskId: 377
ComplianceId: 1793
RiskTitle: Operational Risk Scenario Analysis Risk
Criticality: High
PossibleDamage: Failure to conduct adequate scenario analysis for operational risks, leading to unmiti
Category: Operational
RiskType: Current
BusinessImpact: Inadequate scenario analysis and stress testing of operational risks, resulting in unas
RiskDescription: Failure to account for operational failures such as system outages or fraud, leading to
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 8
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: Enhance operational risk scenario testing, integrate emerging risks such as cyber threa
CreatedAt: 2025-08-12 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2721:
RiskId: 376
ComplianceId: 1792
RiskTitle: Credit Risk Capital Adequacy Compliance Incident
Criticality: Critical
PossibleDamage: Inadequate capital reserves to meet credit risk requirements, leading to regulatory n
Category: Operational
RiskType: Current
BusinessImpact: Failure to maintain required capital for credit risk exposures, potentially leading to fina
RiskDescription: Underestimation of credit risk exposure, resulting in inadequate capital buffers and po
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 9
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Ensure credit risk models are updated, increase capital buffers, review internal risk mar
CreatedAt: 2025-08-11 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: IT Operations Unit
Item 2722:
RiskId: 375
ComplianceId: 1791
RiskTitle: Collateral & Margin Requirements Risk
Criticality: Critical
PossibleDamage: Non-compliance with collateral and margining requirements, resulting in increased c
Category: Operational
RiskType: Current
BusinessImpact: Failure to comply with collateral and margining standards, leading to insufficient cove
RiskDescription: Inadequate margining and collateral management, exposing the bank to counterparty

RiskLikelihood: 9
RiskImpact: 10
RiskExposureRating: 9
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Implement daily margining requirements, update collateral management procedures, ar
CreatedAt: 2025-08-10 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division

Item 2723:
RiskId: 374
ComplianceId: 1790
RiskTitle: Portfolio & Credit Stress Testing Risk
Criticality: High
PossibleDamage: Failure to conduct appropriate credit stress testing for loan portfolios, leading to una
Category: Operational
RiskType: Current
BusinessImpact: Inadequate stress testing of loan portfolios under adverse conditions, leading to unqu
RiskDescription: Failure to assess the impact of adverse economic conditions on the credit portfolio, re
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 8
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Ensure quarterly stress tests on loan portfolios, update scenarios for credit defaults and
CreatedAt: 2025-08-09 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Core Banking IT
BusinessUnitName: Compliance Division

Item 2724:
RiskId: 373

ComplianceId: 1789
RiskTitle: Counterparty Credit Risk Derivative Exposure Risk
Criticality: Critical
PossibleDamage: Non-compliance with counterparty credit risk capital requirements, leading to exposu
Category: Operational
RiskType: Current
BusinessImpact: Failure to properly calculate and mitigate counterparty risk exposure from derivatives,
RiskDescription: Inadequate collateral management and exposure limits, increasing risk during counte
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 9
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Review counterparty credit risk exposure models, increase collateral management for c
CreatedAt: 2025-08-08 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Compliance Division

Item 2725:
RiskId: 372
ComplianceId: 1788
RiskTitle: Macroeconomic Stress Testing Risk
Criticality: High
PossibleDamage: Failure to conduct appropriate stress tests for macroeconomic conditions, leading to
Category: Operational
RiskType: Current
BusinessImpact: Failure to account for extreme but plausible economic scenarios, leading to capital sh
RiskDescription: Inadequate stress testing scenarios for macroeconomic shocks, resulting in potential
RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 8
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1

RiskPriority: Medium

RiskMitigation: Implement quarterly stress tests for extreme macroeconomic scenarios, strengthen sce

CreatedAt: 2025-08-07 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Information Security

BusinessUnitName: IT Operations Unit

Item 2726:

RiskId: 371

ComplianceId: 1787

RiskTitle: Pillar 3 Public Disclosure Risk

Criticality: High

PossibleDamage: Inadequate public disclosures of risk exposures and capital adequacy, resulting in re

Category: Operational

RiskType: Current

BusinessImpact: Failure to disclose risk-weighted assets, capital ratios, and exposure profiles, leading

RiskDescription: Inaccurate or incomplete public disclosures, risking regulatory penalties and loss of in

RiskLikelihood: 8

RiskImpact: 9

RiskExposureRating: 9

RiskMultiplierX: 0.1

RiskMultiplierY: 0.1

RiskPriority: High

RiskMitigation: Ensure full and accurate disclosure of capital adequacy, risk-weighted assets, and risk

CreatedAt: 2025-08-06 00:00:00

CreatedBy: System

CreatedByName: System User

DepartmentName: Core Banking IT

BusinessUnitName: Compliance Division

Item 2727:

RiskId: 370

ComplianceId: 1786

RiskTitle: Leverage Ratio Risk

Criticality: Medium

PossibleDamage: Failure to maintain the required leverage ratio, leading to underreporting of financial

Category: Operational
RiskType: Current
BusinessImpact: Inadequate capital to absorb financial leverage risks, increasing exposure to systemic
RiskDescription: Incorrect calculation of the leverage ratio, leading to regulatory non-compliance and c
RiskLikelihood: 6
RiskImpact: 7
RiskExposureRating: 8
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: Review and update leverage ratio models, ensure full inclusion of off-balance-sheet exp
CreatedAt: 2025-08-05 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: IT Operations Unit

Item 2728:
RiskId: 369
ComplianceId: 1785
RiskTitle: Net Stable Funding Ratio Risk
Criticality: High
PossibleDamage: Failure to maintain sufficient stable funding over a one-year horizon, leading to long-
Category: Operational
RiskType: Current
BusinessImpact: Inability to meet the required NSFR, resulting in long-term funding shortages and incr
RiskDescription: Shortage of stable funding sources, increasing the risk of liquidity shortfalls under pro
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 9
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Increase stable funding sources, reduce reliance on short-term funding, update NSFR c
CreatedAt: 2025-08-04 00:00:00
CreatedBy: System

CreatedByName: System User
DepartmentName: Information Security
BusinessUnitName: Retail Banking
Item 2729:
RiskId: 368
ComplianceId: 1784
RiskTitle: Liquidity Coverage Ratio Risk
Criticality: Critical
PossibleDamage: Failure to meet liquidity requirements, potentially leading to inability to meet short-te
Category: Operational
RiskType: Current
BusinessImpact: Inadequate liquidity to cover net cash outflows during a 30-day stress period, leading
RiskDescription: Failure to maintain HQLA reserves in alignment with Basel III liquidity standards.
RiskLikelihood: 9
RiskImpact: 10
RiskExposureRating: 9
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Reassess liquidity stress scenarios, ensure HQLA reserves meet LCR requirements, im
CreatedAt: 2025-08-03 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Compliance Division
Item 2730:
RiskId: 367
ComplianceId: 1783
RiskTitle: Market & Operational Risk Capital Risk
Criticality: High
PossibleDamage: Failure to maintain adequate capital buffers to absorb potential losses from market fl
Category: Operational
RiskType: Current
BusinessImpact: Inability to absorb market volatility or operational failures leading to liquidity or financi
RiskDescription: Underestimation of market or operational risk exposure, resulting in capital inadequac

RiskLikelihood: 7
RiskImpact: 8
RiskExposureRating: 8
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: Medium
RiskMitigation: Increase capital buffers, review stress tests for market and operational risk, strengthen
CreatedAt: 2025-08-02 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Risk Management
BusinessUnitName: Retail Banking

Item 2731:
RiskId: 366
ComplianceId: 1782
RiskTitle: Credit Risk Capital Adequacy Risk
Criticality: Critical
PossibleDamage: Inability to meet regulatory capital requirements for credit risk, resulting in regulatory
Category: Operational
RiskType: Current
BusinessImpact: Failure to maintain adequate capital to cover credit risk exposures, leading to financia
RiskDescription: Inaccurate RWA calculation leading to capital shortfalls and failure to meet Basel III st
RiskLikelihood: 8
RiskImpact: 9
RiskExposureRating: 9
RiskMultiplierX: 0.1
RiskMultiplierY: 0.1
RiskPriority: High
RiskMitigation: Update risk models, ensure capital reserves meet Basel III requirements, improve gove
CreatedAt: 2025-08-01 00:00:00
CreatedBy: System
CreatedByName: System User
DepartmentName: Customer Service
BusinessUnitName: Retail Banking