# Risk Register – PDF (Synthetic Test Data)

Risk 1: Unmonitored Admin Console Access from Public Network (PDF)
Description: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to unauthorize
d access, service disruption, or regulatory non■compliance. Preliminary evidence from logs and change tickets
indicates exposure windows in the last quarter.
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust erosion,
and operational downtime affecting critical processes.
Priority: High  Criticality: Medium  Category: Operational
Origin: Incident  Likelihood: 4  Impact: 5
Response: Mitigate  Owner: anil.kumar
Status (may be missing):  BusinessImpact (may be missing):
DueDate: 2025-10-12  Reviewer: qa.lead
Mitigation (JSON): {"1": "Implement control hardening per standard", "2": "Enable continuous monitoring with a
lerting thresholds", "3": "Review access and rotate credentials; enforce MFA where applicable"}
—

Risk 2: Shadow IT File-Sharing Tools Cause Data Leakage (PDF)
Description: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to unauthorize
d access, service disruption, or regulatory non■compliance. Preliminary evidence from logs and change tickets
indicates exposure windows in the last quarter.
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust erosion,
and operational downtime affecting critical processes.
Priority: Low  Criticality: Medium  Category: Technology Risk
Origin: PenTest  Likelihood: 1  Impact: 3
Response: Mitigate  Owner: radha.sharma
Status (may be missing):  BusinessImpact (may be missing):
DueDate: 2025-06-16  Reviewer: ciso
Mitigation (JSON): {"1": "Implement control hardening per standard", "2": "Enable continuous monitoring with a
lerting thresholds", "3": "Review access and rotate credentials; enforce MFA where applicable"}
—

Risk 3: Unauthorized API Access Due to Token Mismanagement (PDF)
Description: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to unauthorize
d access, service disruption, or regulatory non■compliance. Preliminary evidence from logs and change tickets
indicates exposure windows in the last quarter.
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust erosion,
and operational downtime affecting critical processes.
Priority: Low  Criticality: Low  Category: Process Risk
Origin: Compliance  Likelihood: 8  Impact: 1
Response: Transfer  Owner: radha.sharma
Status (may be missing):  BusinessImpact (may be missing):

DueDate: 2025-11-24  Reviewer: it.audit
Mitigation (JSON): {"1": "Implement control hardening per standard", "2": "Enable continuous monitoring with alerting thresholds", "3": "Review access and rotate credentials; enforce MFA where applicable"}
—

Risk 4: Misconfigured S3 Bucket Exposes Confidential Reports (PDF)
Description: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to unauthorized access, service disruption, or regulatory non■compliance. Preliminary evidence from logs and change tickets indicates exposure windows in the last quarter.
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust erosion, and operational downtime affecting critical processes.
Priority: High  Criticality: Low  Category: Process Risk
Origin: Compliance  Likelihood: 9  Impact: 9
Response: Avoid  Owner: sagar.patil
Status (may be missing):  BusinessImpact (may be missing):
DueDate: 2025-11-10  Reviewer: it.audit
Mitigation (JSON): {"1": "Implement control hardening per standard", "2": "Enable continuous monitoring with alerting thresholds", "3": "Review access and rotate credentials; enforce MFA where applicable"}
—

Risk 5: Weak Vendor VPN Authentication Causes Lateral Movement Risk (PDF)
Description: This risk arises from gaps in controls and monitoring. If unaddressed, it may lead to unauthorized access, service disruption, or regulatory non■compliance. Preliminary evidence from logs and change tickets indicates exposure windows in the last quarter.
PossibleDamage: Potential impacts include confidentiality breach, financial penalties, customer trust erosion, and operational downtime affecting critical processes.
Priority: High  Criticality: Medium  Category: Operational
Origin: Incident  Likelihood: 1  Impact: 7
Response: Avoid  Owner: sagar.patil
Status (may be missing):  BusinessImpact (may be missing):
DueDate: 2025-10-28  Reviewer: qa.lead
Mitigation (JSON): {"1": "Implement control hardening per standard", "2": "Enable continuous monitoring with alerting thresholds", "3": "Review access and rotate credentials; enforce MFA where applicable"}
—