ENTERPRISE RISK MANAGEMENT

CONFIDENTIAL — INTERNAL USE

THIRD-PARTY RISK MANAGEMENT

End-to-End Vendor Risk Management Program

Automated Risk Register — Executive Dashboards — Audit Readiness

01 — FRAMEWORK

Enterprise Vendor Risk Framework

Aligned with ISO 27001 & NIST CSF standards

02 — AUTOMATION

Automated Risk Register

Factor-based scoring: Inherent to Residual risk

03 — REPORTING

Executive Dashboards

High-risk vendors, overdue reviews, audit-ready visuals

04 — GOVERNANCE

Governance & Compliance

RACI ownership, SLAs, audit-defensible decisions

ALIGNED WITH — ISO 27001 | NIST CSF | GRC Maturity

Cloud-Ready

Power BI / SharePoint / Power Automate

Risk Scoring

Inherent / Control / Residual Risk

Audit-Ready

Evidence Links / Certification Tracking

● Arshman Abbas
GRC — RISK MANAGEMENT

● Jarrar Hassan
CYBERSECURITY — COMPLIANCE

2025

v1.0 — ENTERPRISE EDITION

Executive Overview

1.1 Background and Business Context

Modern organizations rely heavily on third-party vendors to deliver critical business capabilities such as cloud infrastructure, payment processing, and enterprise collaboration. While these vendors enable scalability, speed, and cost efficiency, they also introduce material risks that are often outside the direct control of the organization.

Third-party vendor risks are no longer limited to technical security failures. They directly impact:

- Confidentiality of customer and business data
- Regulatory and compliance obligations
- Operational continuity and service availability
- Brand reputation and customer trust

> **Industry Context:** Recent industry incidents demonstrate that vendor-related failures can result in data breaches, service outages, regulatory penalties, and long-term reputational damage. As a result, vendor risk has become a board-level concern rather than a purely technical issue.

1.2 Business Impact of Third-Party Vendor Risk

Unmanaged or poorly governed vendor risk can have significant business consequences, including:

Financial Impact

Regulatory fines, incident response costs, legal exposure, and revenue loss due to service disruption.

Operational Impact

Dependency on vendors for critical services increases the likelihood of cascading failures if vendors lack resilience.

Compliance Impact

Failure of vendors to meet security or privacy requirements can place the organization in direct violation of regulatory standards.

Strategic Impact

Vendor incidents can delay business initiatives, product launches, and partnerships.

Because vendors often operate outside the organization's direct control, these risks require a structured governance model rather than ad-hoc assessments.

1.3 Purpose of the Vendor Risk Assessment Framework

The purpose of this Enterprise Third-Party Vendor Risk Assessment Framework is to provide a consistent, repeatable, and risk-based approach for evaluating and managing risks introduced by third-party vendors.

This framework enables the organization to:

- Identify and assess vendor risks in a standardized manner
- Compare vendors using objective risk criteria
- Support informed business decisions regarding vendor onboarding, continuation, or termination
- Establish accountability for vendor-related risks across business and security functions
- Demonstrate due diligence to auditors, regulators, and senior management

> **Framework Philosophy:** The framework is designed to support decision-making, not just documentation. It focuses on material risks that affect business outcomes rather than technical control checklists.

1.4 Framework Enablement and Value

This framework enables effective vendor risk management by integrating governance, risk assessment, and executive oversight into a single operating model.

Key enablement outcomes include:

- **Risk visibility:** Clear understanding of which vendors pose the highest risk and why
- **Decision clarity:** Defined criteria for accepting, mitigating, or rejecting vendor risks
- **Ownership and accountability:** Clear assignment of risk ownership and escalation paths
- **Audit readiness:** Documented processes and evidence supporting vendor risk decisions

- **Scalability:** Ability to assess new vendors consistently as the organization grows

Governance Model - Three Lines of Defense

This GRC framework is aligned with the Three Lines of Defense (3LoD) model to ensure effective governance, accountability, and independence across risk management activities.

- The **First Line of Defense** consists of business and vendor owners who are responsible for day-to-day risk ownership and execution of security controls.
- The **Second Line of Defense** is represented by the GRC and Risk Management function, which defines policies, establishes risk assessment methodologies, performs independent risk reviews, and monitors control effectiveness.
- The **Third Line of Defense** is Internal Audit, which provides independent assurance on the adequacy and effectiveness of governance, risk management, and internal controls.

This model ensures clear segregation of duties and aligns the framework with enterprise and regulatory expectations

1.5 Key Stakeholders and Governance Bodies

Effective vendor risk management requires collaboration between business, security, and governance functions. This framework is designed to support the following key stakeholders:

STAKEHOLDER	ROLE IN FRAMEWORK
Chief Information Security Officer (CISO)	Provides oversight of vendor cybersecurity risk, ensures alignment with the organization's security strategy, reviews high-risk vendor assessments and control gaps
Risk Committee	Provides independent oversight of material vendor risks, approves risk acceptance decisions above defined thresholds, ensures vendor risks align with the organization's risk appetite

Business Owners	Own the vendor relationship and business dependency, participate in risk assessment and remediation planning, accept residual risk where appropriate
Legal and Compliance	Assess regulatory, contractual, and privacy obligations, ensure vendor agreements include appropriate risk controls

1.6 Executive Summary Statement

Framework Value Proposition: This framework establishes a formal, enterprise-level approach to managing third-party vendor risk. By aligning vendor risk assessment with business impact, governance, and executive oversight, the organization strengthens its ability to make informed, defensible decisions while supporting secure and compliant business growth.

Scope & Applicability

2.1 Purpose of Scope Definition

The purpose of this section is to clearly define where the Third-Party Vendor Risk Assessment Framework applies and where it does not. Establishing a well-defined scope ensures that vendor risk assessments remain consistent, relevant, and focused on material business risks.

This framework is designed to prioritize vendors that pose meaningful cybersecurity, compliance, or operational risk to the organization, rather than attempting to assess all vendors equally.

2.2 In-Scope Vendor Types

This framework applies to third-party vendors that meet one or more of the following criteria:

- Store, process, or transmit organizational data
- Have logical or physical access to internal systems or networks
- Support business-critical or customer-facing services
- Provide infrastructure or platforms on which key business operations depend

Primary In-Scope Vendor Categories

- **Cloud Service Providers**

Vendors providing infrastructure, platforms, or software services that host or process organizational data.

- **Payment Gateways and Financial Service Providers**

Vendors involved in payment processing, financial transactions, or handling of sensitive financial data.

- **Email, Collaboration, and Productivity Platforms**

Vendors enabling communication, document storage, and collaboration across the organization.

These categories represent vendors with the highest potential business and security impact and therefore require formal risk assessment.

2.3 In-Scope Risk Domains

The framework evaluates vendor risk across six fixed risk domains. These domains represent the minimum set of risk areas required to support informed vendor decisions:

RISK DOMAIN	DESCRIPTION
Data Protection	Safeguards for data confidentiality, integrity, and encryption
Identity and Access Management	Control of user access, authentication, and authorization
Compliance and Privacy	Alignment with regulatory, contractual, and privacy requirements
Business Continuity	Resilience, availability, and disaster recovery capabilities
Incident Response	Detection, response, and communication during security incidents
Vendor Governance	Policies, oversight, and accountability within the vendor organization

Supply Chain & nth-Party	Evaluates vendor dependency on sub-service organizations (fourth-parties) and their internal processes for managing downstream providers.

> **Domain Consistency:** These domains are intentionally fixed to ensure consistency and comparability across vendor assessments.

2.4 Applicability Across the Vendor Lifecycle

This framework applies at multiple stages of the vendor lifecycle, including:

- **Pre-onboarding:** Risk assessment prior to contract execution
- **Ongoing operations:** Periodic reassessment of active vendors
- **Change events:** Significant changes in vendor services, scope, or risk profile
- **Contract renewal or termination:** Re-evaluation of vendor risk prior to renewal decisions

Risk assessment frequency and depth may vary based on vendor criticality and risk level.

2.5 Out-of-Scope Exclusions

The following vendor types and scenarios are explicitly excluded from this framework unless otherwise approved by the Risk Committee:

- Vendors with no access to organizational systems or data
- Low-risk suppliers providing non-digital or commoditized services
- Individual contractors operating under direct organizational supervision
- One-time vendors with no ongoing service or data exposure

Exclusions are documented to prevent unnecessary assessment effort and to maintain focus on material risk.

2.6 Assumptions and Constraints

The framework operates under the following assumptions:

- Vendor-provided information is subject to validation where feasible
- Risk assessments are based on available evidence at the time of review
- Not all vendor risks can be eliminated; residual risk is expected
- Business needs may require risk acceptance with appropriate approvals

These assumptions support pragmatic, risk-based decision-making rather than absolute risk elimination.

2.7 Scope Governance

Any exceptions to the defined scope must be formally reviewed and approved by the Risk Committee. Scope changes driven by regulatory requirements, business expansion, or emerging threats will be incorporated through periodic framework review.

Governance & Ownership

3.1 Governance Objective

The objective of the governance and ownership model is to ensure that third-party vendor risks are clearly owned, appropriately reviewed, and formally decided at the correct level of the organization.

> **Core Principle:** This framework establishes accountability for vendor risk decisions while ensuring that business, security, and compliance stakeholders are actively involved. No vendor risk is accepted by default; all risk acceptance must be deliberate, documented, and approved.

3.2 Roles and Responsibilities

Vendor risk management is a shared responsibility across multiple functions. The following roles are defined to ensure clear accountability:

ROLE	KEY RESPONSIBILITIES
Business Owner	Owns the relationship with the vendor; Understands the business dependency and criticality of the vendor; Participates in risk remediation planning; Accepts residual risk where authorized
Risk Owner	Accountable for managing identified vendor risks; Ensures risks are tracked, reviewed, and updated; Coordinates mitigation actions across teams
Information Security	Conducts vendor risk assessments; Reviews security controls and evidence; Advises on risk severity and control gaps
Legal and Compliance	Reviews regulatory, contractual, and privacy requirements; Ensures vendor agreements include appropriate risk clauses; Advises on compliance-related risk exposure

Risk Committee	Provides oversight of material and high-risk vendors; Reviews and approves risk acceptance decisions; Resolves escalated vendor risk issues

3.3 Roles & Responsibilities (R&R) Matrix

The table below summarizes accountability across key vendor risk activities:

ACTIVITY	Vendor Onboarding	Risk Assessment	Risk Mitigation	Risk Acceptance	Contract Approval	Periodic Review
BUSINESS OWNER	**A**	**C**	**A**	**A**	**C**	**C**
RISK OWNER	**R**	**R**	**R**	**C**	**I**	**R**
INFOSEC	**C**	**A**	**C**	**C**	**C**	**A**
LEGAL & COMPLIANCE	**C**	**C**	**C**	**C**	**A**	**C**
RISK COMMITTEE	**I**	**I**	**I**	**A**	**I**	**I**

Legend: **A** = Accountable | **R** = Responsible | **C** = Consulted | **I** = Informed

3.4 Decision Authority Matrix (RAM)

Vendor risk decisions are based on the level of residual risk identified during assessment.

RESIDUAL RISK LEVEL	DECISION AUTHORITY	REQUIRED ACTION
LOW	Business Owner	Accept
MEDIUM	Business Owner + Risk Owner	Accept with controls
HIGH	Risk Committee	Mitigate or Reject

This matrix ensures that higher-risk decisions receive appropriate executive oversight.

3.5 Escalation Logic

Vendor risks must be escalated under the following conditions:

- Residual risk exceeds defined risk appetite
- Critical control gaps are identified with no feasible mitigation
- Vendor experiences a significant security incident
- Regulatory or contractual non-compliance is identified

Escalated risks are reviewed by the Risk Committee, which determines whether to:

- Approve risk acceptance
- Require additional mitigation
- Suspend or terminate the vendor relationship

3.6 Risk Ownership Principles

The following principles apply to all vendor risk decisions:

- Risk ownership cannot be delegated to vendors
- Risk acceptance requires explicit approval
- Business urgency does not override governance
- All decisions must be documented and auditable

These principles ensure consistent and defensible vendor risk management across the organ

Vendor Risk Lifecycle (Onboarding to Secure Offboarding)

4.1 Lifecycle Objective

The Vendor Risk Lifecycle defines a structured, end-to-end process for identifying, assessing, managing, and monitoring risks associated with third-party vendors. The objective is to ensure that vendor risk is evaluated consistently throughout the vendor relationship and not treated as a one-time activity.

This lifecycle integrates risk assessment into business processes, enabling timely decision-making while maintaining governance and oversight.

4.2 Overview of the Vendor Risk Lifecycle

The vendor risk lifecycle consists of five key stages:

1. **Vendor Onboarding**

Initial vendor identification and scope determination

2. **Risk Identification and Assessment**

Formal risk evaluation across defined domains

3. **Risk Treatment and Decision**

Determination of risk mitigation and acceptance

4. **Contract Execution and Enablement**

Contractual control implementation and vendor activation

5. **Ongoing Monitoring and Review**

Continuous risk monitoring and periodic reassessment

Each stage includes defined entry and exit criteria to ensure accountability and control.

6. **Secure Off boarding**

4.3 Stage 1: Vendor Onboarding

Purpose:

To formally initiate vendor engagement and determine whether a vendor requires a risk assessment.

Entry Criteria:

- New vendor proposed by a business unit
- Change in scope for an existing vendor
- Renewal of an existing vendor contract

Key Activities:

- Identification of vendor type and service provided
- Preliminary assessment of data access and system exposure
- Assignment of Business Owner and Risk Owner

Exit Criteria:

- Vendor classified as in-scope or out-of-scope
- Decision to proceed with formal risk assessment

4.4 Stage 2: Risk Identification and Assessment

Purpose:

To identify and assess risks introduced by the vendor across defined risk domains.

Key Activities:

- Distribution of vendor risk questionnaire
- Review of vendor responses and supporting evidence
- Assessment across six fixed risk domains
- Calculation of inherent and residual risk

Outputs:

- Documented risk statements
- Preliminary risk ratings

- Identified control gaps

Risk Appetite and Risk Tolerance

The organization defines a formal risk appetite to ensure that risk exposure remains aligned with business objectives and regulatory requirements.

Risk tolerance thresholds are applied to guide decision-making and escalation.

• **Low residual risks** may be accepted by the business owner.
• **Medium residual risks** require management review and approval.
• **High residual risks** require executive-level approval or escalation to a risk committee.

This approach ensures consistent, transparent, and accountable risk acceptance decisions across the organization.

4.5 Stage 3: Risk Treatment and Decision

Purpose:

To determine how identified risks will be managed prior to vendor approval or continuation.

Key Activities:

- Evaluation of mitigation options
- Agreement on remediation actions and timelines
- Determination of residual risk
- Formal risk decision (accept, mitigate, transfer, or reject)

Decision Authority: Risk decisions follow the Decision Authority Matrix defined in Section 3.

Exit Criteria:

- Approved risk treatment plan
- Documented risk acceptance or rejection

4.6 Stage 4: Contract Execution and Enablement

Purpose:

To ensure that risk treatment decisions are reflected in contractual and operational controls.

Key Activities:

- Inclusion of security and compliance requirements in contracts
- Definition of incident notification and audit rights
- Confirmation of service-level and continuity commitments

Exit Criteria:

- Contract execution with risk-aligned controls
- Vendor enabled for operational use

4.7 Stage 5: Ongoing Monitoring and Review

Purpose:

To ensure that vendor risk remains within acceptable levels throughout the relationship.

Key Activities:

- Periodic reassessment based on vendor risk level
- Review of incidents, breaches, or service disruptions
- Monitoring of regulatory or business changes
- Update of risk register and evidence

Review Frequency:

VENDOR RISK LEVEL	REVIEW FREQUENCY
HIGH	At least annually
MEDIUM	Every 18–24 months
LOW	As required

4.8 Stage 6: Secure Off Boarding

Secure offboarding ensures that termination of third-party services does not introduce residual security, privacy, or compliance risk. When a vendor relationship ends—due to contract expiration, service replacement, or risk-based termination—the organization performs a controlled exit to ensure data protection and access removal.

Key Secure Offboarding Activities include:

- Verification that all organizational data has been returned or securely destroyed
- Confirmation of data deletion in accordance with NIST SP 800-88 guidance
- Revocation of user, administrative, and API access
- Termination of integrations and network connectivity
- Retrieval or confirmed destruction of organizational assets
- Completion of secure offboarding activities is required before a vendor relationship is formally closed.

4.8 Lifecycle Governance and Exceptions

Any deviations from the defined lifecycle, including expedited onboarding or temporary risk acceptance, must be documented and approved by the appropriate authority. Lifecycle exceptions are reviewed periodically to ensure they do not become permanent control gaps.

Risk Methodology

5.1 Methodology Objective

The objective of the vendor risk methodology is to provide a consistent, objective,and repeatable approach for identifying, assessing, and comparing risks introduced by third-party vendors.

This methodology is designed to support business-aligned decision-making by translating technical and operational control information into measurable risk outcomes that can be understood by both technical and non-technical stakeholders.

5.2 Risk Domain Model

Vendor risk is assessed across six fixed risk domains. These domains represent the minimum risk coverage required to evaluate a vendor's ability to securely and reliably support organizational operations.

> **Domain Consistency:** The use of fixed domains ensures consistency, comparability, and governance across all vendor assessments.

Defined Risk Domains

1. **Data Protection**

Measures the vendor's ability to protect data confidentiality, integrity, and availability through encryption, data handling practices, and data life cycle controls.

2. **Identity and Access Management**

Evaluates how access to systems and data is authenticated, authorized, and reviewed, including privileged access controls.

3. **Compliance and Privacy**

Assesses alignment with regulatory, legal, and contractual requirements, including privacy obligations and audit readiness.

4. **Business Continuity**

Examines resilience, availability, disaster recovery capabilities, and the vendor's ability to sustain operations during disruptions.

5. **Incident Response**

Reviews the vendor's ability to detect, respond to, communicate, and recover from security incidents in a timely manner.

6. **Vendor Governance**

Evaluates internal security governance, policy enforcement, risk management practices, and executive oversight within the vendor organization.

7 . **Supply Chain & Nth-Party Risk**

Measures the potential for cascading failures caused by the vendor's critical subcontractors, such as cloud infrastructure providers (e.g., AWS, Azure) or sub-processors of sensitive data. This domain ensures that the vendor's risk management practices extend to their own supply chain to prevent "blind spots" in the organization's security posture.

5.3 Assessment Technique

Vendor risk assessments are conducted using a structured questionnaire supported by evidence validation.

Assessment Components

- Multiple-choice questions mapped to each risk domain
- Scoring scale from 1 to 5 based on control effectiveness
- Evidence requirements to support vendor responses

The assessment focuses on control maturity and operational effectiveness

5.4 Scoring Model

Control Scoring Scale

SCORE	DESCRIPTION
5	Control fully implemented and consistently effective
4	Control implemented with minor gaps
3	Control partially implemented
2	Control largely ineffective
1	Control not implemented

5.5 Inherent Risk Determination

Inherent risk represents the level of risk posed by a vendor in the absence of controls.

Inherent risk is determined using two factors:

- **Likelihood** – Probability of a risk event occurring
- **Impact** – Potential business impact if the risk materializes

Formula:

Inherent Risk = Likelihood × Impact

Likelihood and impact are rated using standardized scales defined by the organization to ensure consistency across assessments.

5.6 Control Effectiveness Evaluation

Control effectiveness reflects how well vendor controls reduce inherent risk.

Control effectiveness is determined by:

- Assessment responses
- Quality and completeness of supporting evidence
- Observed control maturity

Higher control effectiveness results in greater reduction of inherent risk.

5.7 Residual Risk Calculation

Residual risk represents the remaining level of risk after accounting for control effectiveness.

Formula:

Residual Risk = Inherent Risk – Control Effectiveness

Residual risk is the primary input for risk treatment and decision-making.

5.8 Risk Rating Normalization

Residual risk scores are normalized into qualitative risk ratings to support management understanding:

RATING	DESCRIPTION
LOW	Risk is within acceptable tolerance
MEDIUM	Risk requires management attention
HIGH	Risk exceeds acceptable tolerance

This normalization enables consistent reporting and escalation across vendors.

5.9 Use of Professional Judgment

While the scoring model provides structure, professional judgment is applied where necessary. Factors such as vendor criticality, business dependency, and external threat intelligence may influence final risk ratings.

Any adjustments based on judgment must be documented to maintain transparency and auditability.

5.10 Methodology Governance

The risk methodology is reviewed periodically to ensure alignment with evolving business needs, regulatory requirements, and threat landscapes. Changes to the methodology require approval from the Risk Committee.

5.11 Cloud Share Responsibility Considerations

For cloud-based service providers, risk assessments must account for the shared responsibility model. While cloud service providers are responsible for the security of the underlying infrastructure, the organization remains responsible for securing data, identities, configurations, and access within the cloud environment. Vendor risk evaluations therefore distinguish between provider-managed controls and customer-managed responsibilities, based on the service delivery model.

Cloud Model	Vendor Responsibility	Organization Responsibility
SaaS	Infrastructure, platform, application	Data, user access, configuration
PaaS	Infrastructure, runtime	Application code, data, access
IaaS	Physical data centers	OS, network config, data, IAM

Risk Classification & Treatment

6.1 Objective of Risk Classification

The objective of risk classification is to translate assessed residual risk into clear, actionable decisions. Risk classification ensures that vendor risks are treated consistently and aligned with the organization's risk appetite.

This section defines how risks are categorized, what actions are required for each category, and who has the authority to approve those actions.

6.2 Risk Classification Levels

Residual risks identified during vendor assessments are classified into the following levels:

RISK LEVEL	DESCRIPTION
LOW	Risk is within acceptable tolerance and does not require additional action
MEDIUM	Risk requires defined controls or monitoring to remain acceptable
HIGH	Risk exceeds acceptable tolerance and requires mitigation or rejection

These classifications provide a common language for communicating risk across technical and non-technical stakeholders.

6.3 Risk Treatment Options

For each identified risk, one of the following treatment options must be selected:

Accept

Acknowledge and formally accept residual risk

Mitigate

Implement additional controls to reduce risk

Transfer

Transfer risk through contractual, insurance, or third-party mechanisms

Avoid

Discontinue or reject the vendor relationship

Risk treatment decisions are documented and tracked through the risk register.

Isssue and Remediation Managment

Identified control gaps are formally logged as issues and tracked through a structured remediation lifecycle.

Each issue is assigned a responsible owner, remediation plan, and target completion date.

Remediation actions are **monitored by the GRC function**, and issues are only closed after validation confirms that the identified risk has been adequately addressed.

This lifecycle ensures accountability, traceability, and continuous improvement of the control environment.

6.4 Decision Logic by Risk Level

RESIDUAL RISK	DEFAULT TREATMENT	APPROVAL REQUIREMENT
LOW	Accept	Business Owner
MEDIUM	Accept with controls	Business Owner + Risk Owner
HIGH	Mitigate or Avoid	Risk Committee

Important: Exceptions to default treatment require formal justification

6.5 Risk Acceptance Principles

Risk acceptance is a conscious business decision and must adhere to the following principles:

- Risk acceptance must be explicit and documented
- Acceptance must be aligned with defined risk appetite
- Temporary risk acceptance must include review dates
- Accepted risks remain subject to ongoing monitoring

Risk acceptance does not eliminate accountability for future incidents.

6.6 Risk Mitigation Planning

When mitigation is required, a documented mitigation plan must be developed that includes:

- Description of required control improvements
- Responsible owner for each action
- Target completion dates
- Verification criteria

Mitigation progress is tracked and reviewed until risk is reduced to an acceptable level.

6.7 Risk Treatment Tracking

All risk treatment decisions and actions are tracked within the centralized risk register. Changes in risk level or treatment status must be supported by updated evidence and reviewed by the appropriate stakeholders.

6.8 Escalation and Reassessment

Risks must be reassessed and escalated if:

- Mitigation actions are delayed or ineffective
- Vendor circumstances change materially
- New threats or vulnerabilities emerge

Reassessment ensures that risk decisions remain valid over time.

6.9 Risk Exceptions and Waiver

In situations where a vendor does not fully meet security or compliance requirements, the organization may grant a formal risk exception. Risk exceptions are time-bound, documented decisions that acknowledge residual risk while allowing business operations to proceed.

Exception Rules:

Element	Requirement
Approval Authority	CISO or Risk Committee
Validity Period	Maximum 6–12 months
Documentation	Risk Acceptance Memo
Review Requirement	Mandatory re-assessment
Tracking	Recorded in Risk Register

Risk waivers do not eliminate risk; they formally transfer accountability to executive leadership.

Risk Register & Evidence Management

7.1 Purpose of the Risk Register

The risk register serves as the centralized system of record for all third-party vendor risks identified through this framework. It provides a structured view of risk status, ownership, decisions, and supporting evidence, enabling transparency and accountability across the organization.

The risk register supports governance, reporting, and audit requirements by ensuring that all vendor risk decisions are documented and traceable.

7.2 Risk Register Structure

Each vendor risk recorded in the risk register must include the following mandatory fields:

FIELD	DESCRIPTION
Vendor Name	Legal name of the third-party vendor
Service Description	Summary of the service provided
Risk Domain	Associated risk domain
Risk Statement	Clear description of the risk
Inherent Risk	Risk level prior to controls
Control Summary	Summary of key mitigating controls
Residual Risk	Risk level after controls
Risk Treatment	Accept, Mitigate, Transfer, or Avoid
Risk Owner	Accountable owner of the risk
Decision Authority	Approving authority
Review Date	Next scheduled review

> **Standardization:** This standardized structure ensures consistency across all vendor risk entries.

7.3 Risk Statement Quality

Risk statements must be written in clear business language and describe:

- The risk event
- The potential impact
- The affected business area

Example Risk Statement:

"Unauthorized access to customer data hosted by the vendor may result in regulatory penalties and loss of customer trust."

Clear risk statements support effective decision-making and escalation.

7.4 Evidence Expectations

Vendor risk assessments must be supported by appropriate evidence to validate control effectiveness.

Acceptable Evidence Examples

- ISO/IEC 27001 certification or statements of applicability
- SOC 1 / SOC 2 reports
- Security policies and procedures
- Penetration test summaries
- Business continuity and disaster recovery test results
- Incident response plans

Evidence should be current, relevant, and proportional to the vendor's risk level.

7.5 Evidence Review and Validation

Evidence is reviewed by Information Security and, where applicable, Legal or Compliance teams. Evidence validation focuses on:

- Relevance to identified risks
- Completeness and coverage
- Recency and validity

- Alignment with vendor responses

Control Gaps: Gaps or inconsistencies in evidence may result in increased residual risk or additional mitigation requirements.

7.6 Review Cadence

Risk register entries are reviewed based on vendor criticality and risk level:

VENDOR RISK LEVEL	REVIEW FREQUENCY
HIGH	At least annually
MEDIUM	Every 18–24 months
LOW	As required or upon material change

Reviews ensure that risk assessments remain current and reflect changes in vendor operations or threat landscape.

7.7 Change Management

Material changes that may trigger a risk reassessment include:

- Expansion of vendor service scope
- Changes in data types or access levels
- Security incidents or breaches
- Regulatory or contractual changes

All changes are documented in the risk register with updated assessments and decisions.

7.8 Audit and Reporting Support

The risk register provides evidence of due diligence and governance during audits, regulatory reviews, and management reporting. All decisions, approvals, and supporting evidence must be retained in accordance with organizational record retention policies.

Security Maturity Model

8.1 Objective of the Maturity Model

The Security Maturity Model provides a structured way to evaluate the overall strength, consistency, and reliability of a vendor's security and risk management practices.

While risk scoring measures current exposure, the maturity model assesses the vendor's ability to sustain effective controls over time. This distinction enables more informed trust decisions, particularly for long-term or high-dependency vendors.

8.2 Maturity Levels Overview

Vendor security maturity is assessed across five defined levels. Each level reflects the degree to which security practices are formalized, managed, and continuously improved.

LEVEL	MATURITY DESCRIPTION
Level 1	Ad-hoc
Level 2	Initial
Level 3	Defined
Level 4	Managed
Level 5	Optimized

The maturity level assigned to a vendor represents an overall assessment based on evidence across risk domains.

8.3 Maturity Level Definitions

Level 1 – Ad-hoc

Security controls are informal, undocumented, or inconsistently applied. Risk management activities are reactive and driven by incidents rather than planning.

Level 2 – Initial

Basic security controls exist but are not consistently implemented or monitored. Responsibilities may be unclear, and evidence of control effectiveness is limited.

Level 3 – Defined

Security policies and procedures are documented and implemented across the organization. Controls are generally followed, and responsibilities are clearly assigned.

Level 4 – Managed

Security controls are actively monitored and measured. Risk management is integrated into operational processes, and continuous improvement practices are in place.

Level 5 – Optimized

Security and risk management are embedded into organizational culture. Controls are continuously improved using metrics, automation, and lessons learned.

8.4 Maturity Assessment Approach

Maturity levels are determined based on:

- Vendor questionnaire responses
- Quality and consistency of evidence
- Observed control effectiveness
- Governance and oversight practices

The maturity assessment is qualitative but structured to ensure consistency across vendors.

8.5 Use of Maturity in Risk Decisions

Maturity levels influence vendor trust and risk treatment decisions as follows:

Assessment Frequency

Vendors with higher maturity may require less frequent reassessment

Risk Elevation

Low maturity may increase residual risk even when controls exist

Strategic Planning

Maturity informs long-term vendor strategy and dependency decisions

Important: Maturity does not replace risk scoring but provides additional context for decision-making.

8.6 Maturity Improvement Expectations

For vendors with low or medium maturity, improvement actions may be required as part of risk mitigation plans. Expectations are proportional to vendor criticality and business dependency.

Progress against maturity improvement actions is reviewed during periodic assessments.

8.7 Governance of the Maturity Model

The maturity model is reviewed periodically to ensure alignment with industry practices, regulatory expectations, and organizational risk tolerance. Any changes to maturity definitions require approval from the Risk Committee.

Standards Alignment

9.1 Purpose of Standards Alignment

The purpose of standards alignment is to demonstrate that the Vendor Risk Assessment Framework is grounded in recognized industry standards while remaining tailored to organizational business needs.

Alignment with international standards supports regulatory compliance, audit readiness, and external assurance without requiring vendors or internal teams to adopt standards verbatim.

9.2 Alignment Approach

This framework aligns conceptually and operationally with the following standards:

ISO/IEC 27001

Information Security Management Systems

NIST Cybersecurity Framework (CSF)

Comprehensive cybersecurity risk management

Alignment is achieved through control mapping and outcome equivalence rather than one-to-one replication of standard controls.

Risk Domain	ISO 27001 Annex A	NIST CSF
Data Protection	A.10 Cryptography	PR.DS
IAM	A.9 Access Control	PR.AC
Incident Response	A.16 Incident Mgmt	RS
Business Continuity	A.17 BCM	RC

9.3 ISO/IEC 27001 Alignment

Vendor-related risks and controls assessed under this framework map to relevant ISO/IEC 27001 Annex A control domains, including but not limited to:

- Information security policies
- Access control
- Cryptography and data protection
- Supplier relationships
- Incident management
- Business continuity and resilience

Framework Support for ISO 27001

The framework supports ISO 27001 requirements by:

- Ensuring supplier risks are identified and assessed
- Requiring appropriate contractual controls
- Supporting evidence-based risk treatment decisions

This alignment allows organizations operating an ISMS to integrate vendor risk assessments into their broader information security governance model.

9.4 NIST Cybersecurity Framework Alignment

The framework aligns with the five core functions of the NIST Cybersecurity Framework:

NIST CSF FUNCTION	FRAMEWORK ALIGNMENT
Identify	Vendor inventory, risk identification, governance
Protect	Assessment of preventive and protective controls
Detect	Evaluation of monitoring and detection capabilities
Respond	Review of incident response readiness and communication

Recover	Business continuity and recovery planning

This alignment ensures vendor risk is addressed across the full cybersecurity lifecycle rather than isolated to preventive controls.

9.5 Use of Standards in Risk Decisions

Standards alignment informs risk assessment and decision-making by:

- Providing a common reference point for control expectations
- Supporting consistent evaluation across vendors
- Enabling communication with regulators and auditors
- Reducing ambiguity in risk treatment decisions

> **Important:** Standards are used as guidance, not as rigid checklists, allowing flexibility based on vendor context and business impact.

9.6 Evidence and Certification Considerations

Vendor certifications and attestations (such as ISO 27001 certification or SOC reports) are considered supporting evidence but do not automatically eliminate risk.

Certification status is evaluated in conjunction with:

- Scope and applicability of the certification
- Identified control gaps
- Vendor maturity and operational practices

This ensures that reliance on certifications remains risk-based rather than assumption-based.

9.7 Governance of Standards Alignment

Standards alignment is reviewed periodically to ensure continued relevance as standards evolve and regulatory expectations change. Updates to alignment logic require approval from the Risk Committee.

Management Reporting & Risk Acceptance

10.1 Objective of Management Reporting

The objective of management reporting is to provide senior leadership with clear, concise, and actionable visibility into third-party vendor risk. Reporting focuses on material risks, business impact, and required decisions rather than technical detail.

Effective reporting enables leadership to understand risk exposure, prioritize mitigation efforts, and make informed decisions aligned with organizational risk appetite.

10.2 Executive Risk Views

Management reporting presents vendor risk information through high-level views designed for executive consumption, including:

- **Risk Posture**

Overall vendor risk posture

- **High-Risk Vendors**

High and medium risk vendors

- **Risk Trends**

Key risk themes and trends

- **Mitigation Actions**

Outstanding mitigation actions

- **Risk Acceptance Decisions**

Risk acceptance decisions requiring approval

These views enable leadership to assess whether vendor risk exposure is increasing, stable, or improving over time.

10.3 Risk Acceptance Framework

Risk acceptance is a formal management decision acknowledging that residual risk remains after controls are applied. Risk may be accepted when:

- Further mitigation is not feasible or cost-effective
- The risk aligns with defined risk appetite
- Business value outweighs residual risk

Risk acceptance decisions must be documented and approved in accordance with governance requirements.

10.4 Risk Acceptance Authority

Authority to accept risk is determined by residual risk level:

RESIDUAL RISK	APPROVAL AUTHORITY
LOW	Business Owner
MEDIUM	Business Owner + Risk Owner
HIGH	Risk Committee

> **Governance Requirement:** Risk acceptance above defined thresholds requires formal review and documented justification.

10.5 Risk Acceptance Documentation

Accepted risks are documented using a formal Risk Acceptance Memo that includes:

- Description of the risk
- Business justification for acceptance
- Residual risk rating
- Duration of acceptance and review date
- Approving authority

This documentation ensures transparency, accountability, and auditability.

10.6 Reporting Frequency and Escalation

Management reporting frequency is based on risk level and business criticality:

VENDOR CATEGORY	REPORTING FREQUENCY
HIGH-RISK VENDORS	Quarterly reporting
MEDIUM-RISK VENDORS	Biannual reporting
LOW-RISK VENDORS	As required

> **Escalation:** Material changes in vendor risk must be escalated promptly outside of regular reporting cycles.

10.7 Use of Reporting in Decision-Making

Management reports are used to support decisions related to:

- **Vendor Lifecycle**

Vendor onboarding and renewal

- **Investment**

Investment in risk mitigation

- **Termination**

Termination or replacement of vendors

- **Risk Appetite**

Adjustment of risk appetite

Reporting ensures that vendor risk is actively managed rather than passively documented.

Conclusion

Framework Summary

This Enterprise Third-Party Vendor Risk Assessment Framework establishes a structured, business-aligned approach for managing risks introduced by third-party vendors. By integrating governance, risk assessment, and executive oversight, the framework enables informed and defensible decision-making across the vendor lifecycle.

Key Framework Outcomes

The framework shifts vendor risk management from ad-hoc assessments to a consistent operating model that prioritizes material risk, accountability, and transparency. It supports secure business growth by enabling the organization to engage vendors with a clear understanding of associated risks and control expectations.

Governance Integration

Clear ownership, decision authority, and escalation paths ensure vendor risks are managed at the appropriate organizational level.

Risk-Based Approach

Standardized methodology enables consistent evaluation and comparison of vendor risks across the organization.

Standards Alignment

Alignment with ISO 27001 and NIST CSF ensures the framework meets industry best practices and regulatory expectations.

Executive Visibility

Management reporting provides leadership with actionable insights to support informed decision-making.

Framework Sustainability

This framework is designed to be scalable and adaptable, allowing it to evolve with changing business needs, regulatory requirements, and threat landscapes. Ongoing review and continuous improvement will ensure that vendor risk management remains effective and aligned with organizational objectives.

Continuous Improvement

The framework will be reviewed periodically to ensure:

- Alignment with evolving regulatory requirements
- Incorporation of emerging threat intelligence
- Adaptation to changing business models and vendor relationships
- Enhancement based on lessons learned and operational feedback

Final Statement

Through alignment with recognized industry standards, defined ownership and decision authority, and a focus on residual risk and acceptance, the framework strengthens the organization's ability to meet regulatory, audit, and stakeholder expectations while enabling secure and compliant business growth.

✓ **Framework Implementation Readiness**

This framework is ready for enterprise deployment.

Organizations implementing this framework should establish appropriate tooling, training, and stakeholder communication to ensure successful adoption and sustained effectiveness.

Deliverable 2

Vendor Risk Questionnaire

Aligned with ISO/IEC 27001, NIST CSF & CISM Practices

Prepared By: Governance, Risk & Compliance (GRC) Function
Assessment Type: Third-Party Vendor Risk Assessment
Usage: Pre-Onboarding & Periodic Review
Document Classification: Internal Use Only
Document Version: 1.2
Last Review Date: __________
Next Review Date: __________
Framework Owner: GRC Function

Executive Summary

Third-party vendors are essential for modern enterprises but introduce cybersecurity, operational, and regulatory risks. This framework provides a structured, risk-based approach to evaluate and manage these risks, supporting informed vendor onboarding, monitoring, and renewal decisions.

Example: A cloud SaaS vendor storing PII must meet encryption, access control, and incident response requirements before onboarding.

The framework aligns with **ISO/IEC 27001 Annex A**, **NIST CSF**, and **CISM principles**, making it suitable for enterprise, cloud, and regulated environments.

1. Introduction

Outsourcing enhances efficiency but introduces risks. Data breaches or downtime caused by vendors remain a top enterprise concern.

This framework enables:

- **Consistent assessment methodology**
- **Audit-ready control scoring**
- **Residual risk quantification** for governance decisions

Tip: Map vendor services to risk appetite to avoid over- or under-estimating risk.

2. Objectives

- Identify cybersecurity, privacy, and operational risks
- Evaluate vendor control design and effectiveness
- Quantify residual risk to support governance decisions
- Enable consistent onboarding, monitoring, and renewal
- Strengthen enterprise-wide Third-Party Risk Management (TPRM)

Example: Payment processor SOC 2 reports should match your organization's services.

3. Scope and Applicability

In Scope:

- Cloud providers (IaaS, PaaS, SaaS)
- Payment processors / financial vendors
- Vendors with access to enterprise systems or sensitive data

Out of Scope:

- Vendors without system/network/data access
- One-time suppliers with no recurring relationship

Assessment Frequency:

- Pre-onboarding
- Annually
- Upon significant service/risk changes

4. Assessment Methodology and Approach

Three-stage approach:

1. **Inherent Risk Profiling** – Risk before controls
2. **Control-Based Assessment** – Evaluate control presence & effectiveness
3. **Residual Risk Determination** – Quantify remaining risk & define treatment

Tip: Include cross-functional stakeholders (IT, Legal, Business) for accurate scoring.

5. Inherent Risk Profiling

Risk Factor	Description	Score (1–4)	Notes / Example
Data Sensitivity	Public → regulated (PII, PHI, financial)		Cloud CRM with PII = high risk
Access Level	No access → privileged/system access		Admin access to core systems = high risk
Business Criticality	Low → mission-critical		Payment processing = mission-critical
Geographic Exposure	Local → cross-border		Cross-border = potential compliance obligations
Regulatory Impact	None → high		GDPR, PCI DSS, HIPAA relevance

Score = Sum of all factor scores

Classification:

Score	Risk Tier
5–8	Low
9–14	Medium
15–20	High

Tip: High-risk vendors require executive approval and enhanced validation.

6. Response Scale & Residual Risk

Response	Description	Score
Compliant	Fully implemented & effective	0
Partially Compliant	Implemented with gaps	2
Non-Compliant	Not implemented / ineffective	4

Residual Risk = Inherent Risk × Average Control Gap Score

Score	Level	Action
0–20	Low	Acceptable
21–45	Medium	Mitigation required
46+	High	Executive risk acceptance or vendor rejection

Tip: Always include evidence (audit report, screenshots, test logs) to validate responses.

7. Vendor Information

Field	Details
Vendor Name	
Service Description	
Data Types Accessed	
Business Owner	
Geographic Location	
Assessment Date	

7. Control-Based Assessment

Domain 1: Governance & Security Management

1. Does the vendor maintain a formally approved Information Security Policy reviewed at least annually by senior management?
2. Are information security roles and responsibilities clearly defined and assigned?
3. Is there a documented risk management process for identifying and treating information security risks?
4. Are security awareness and training programs conducted for employees on a regular basis?
5. Are third-party risks governed through formal vendor management procedures?

Domain 2: Identity & Access Management

6. Is multi-factor authentication enforced for privileged and remote access?
7. Are access rights provisioned based on the principle of least privilege?
8. Are user access rights reviewed periodically and revoked upon termination or role change?
9. Are shared or generic user accounts prohibited or strictly controlled?
10. Are privileged access activities logged and monitored?

Domain 3: Data Protection & Privacy

11. Is sensitive or customer data encrypted at rest and in transit using industry-accepted standards?
12. Are data classification and handling requirements formally documented and enforced?
13. Are data retention and secure disposal procedures defined and followed?
14. Are applicable privacy and data protection regulations formally identified and addressed?
15. Are controls implemented to prevent unauthorized data exfiltration?
16. Is access to sensitive data restricted based on business need?

Domain 4: Incident Response & Monitoring

17. Does the vendor maintain a documented Incident Response Plan?
18. Are security incidents logged, tracked, and investigated in a timely manner?
19. Has the Incident Response Plan been tested or exercised within the last 12 months?
20. Are customers notified of security incidents in accordance with contractual or regulatory requirements?
21. Are monitoring and alerting mechanisms implemented to detect security incidents?

Domain 5: Business Continuity & Resilience

22. Are business continuity and disaster recovery plans formally documented?
23. Are backup and recovery procedures tested periodically?
24. Are Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) defined and approved?
25. Are critical systems protected against single points of failure?
26. Are third-party dependencies considered in continuity planning?

Domain 6: Compliance, Audit & Legal

27. Does the vendor undergo independent security or compliance audits (e.g., ISO 27001, SOC 2)?
28. Are audit findings tracked and remediated in a timely manner?
29. Are contractual security and compliance obligations formally defined and enforced?
30. Is the vendor subject to regulatory oversight relevant to the services provided?

Domain 7: Cloud / Shared Responsibility (Optional – for SaaS/IaaS Vendors)

31. Has the vendor clearly defined the shared responsibility model between themselves and the customer?
32. Is tenant isolation enforced to prevent cross-customer data access?
33. Are logs integrated with a SIEM solution (e.g., Microsoft Sentinel) for monitoring and incident response?
34. Can data residency be configured to meet geographic or regulatory requirements?

Tip: This domain is crucial for cloud/SaaS/IaaS vendors and ensures regulatory, security, and monitoring compliance

Domain 8: Supply Chain & Nth-Party Management

35. Does the vendor maintain a formal inventory of critical sub-service organizations (fourth-parties) used to deliver the contracted services?
36. Are fourth-party dependencies and their associated risks included in the vendor's annual Business Continuity and Disaster Recovery testing?
37. Does the vendor require their subcontractors to adhere to security and privacy standards (e.g., ISO 27001, SOC 2) equivalent to those required by this organization?
38. Is there a defined process for the vendor to notify the organization if they change a critical sub-processor or fourth-party provider?

9. Assessment Output

- Overall vendor risk rating
- Key control deficiencies
- Business impact summary
- Recommended risk treatment (Accept/Mitigate/Transfer/Avoid)
- Approval authority defined

10. Control Effectiveness Evaluation

Control effectiveness is evaluated using a multi-dimensional approach aligned with audit and assurance best practices.

Each control is assessed across the following dimensions:

• **Design Effectiveness** – Whether the control is appropriately designed to mitigate the identified risk.
• **Operating Effectiveness** – Whether the control is operating consistently and as intended over time.
• **Evidence Quality** – Whether sufficient and verifiable evidence exists to support control operation.

The final control score is calculated as an average of these dimensions, ensuring a realistic and auditable assessment of control strength.

11. Governance & Review

- Reviewed by GRC function
- Medium/High risk → remediation plan
- High risk → executive approval
- Records retained for audits/regulatory purposes

12. Declaration

Vendor confirms information is accurate and complete.

Authorized Representative

Name:
Title:
Signature:
Date:

Case Study:

Third-Party SaaS Vendor Risk Assessment

Vendor Overview

The organization engaged a third-party cloud-based Customer Relationship Management (CRM) Software-as-a-Service (SaaS) provider to support customer engagement and sales operations. The vendor processes and stores customer personally identifiable information (PII), including names, email addresses, and transaction history.

Due to the nature of the data and the vendor's integration with internal business systems, the engagement was classified as a high-impact third-party relationship.

Inherent Risk Assessment

An inherent risk assessment was conducted prior to onboarding using the standardized risk scoring model.

Risk Factor	Description	Score
Data Sensitivity	Storage and processing of customer PII	5
Network Access	API-based integration with internal systems	4
Business Criticality	Sales operations heavily dependent on service availability	4

Total Inherent Risk Score: 13 (High)

The inherent risk was classified as **High** due to sensitive data handling and business reliance on the vendor's service.

Control Assessment and Risk Mitigation

The vendor's control environment was assessed using a structured questionnaire and evidence review process.

Key controls reviewed included:

- Data encryption at rest and in transit
- Role-based access control and multi-factor authentication
- Security monitoring and incident response procedures
- Independent assurance through SOC 2 Type II reporting

Control effectiveness was evaluated across design, operating effectiveness, and evidence quality. The vendor demonstrated strong security controls; however, minor gaps were identified in security monitoring alert timelines and periodic access review documentation.

Average Control Effectiveness Score: 4 (Strong)

Residual Risk Determination

Residual risk was calculated by factoring control effectiveness into the inherent risk score.

Following control mitigation, the residual risk rating was reduced from **High** to **Medium**. While the vendor maintained a mature security posture, residual risk remained due to ongoing exposure of customer PII and external dependency on the SaaS platform.

Risk Treatment Decision

Given the business criticality of the service and the strength of existing controls, the residual risk was **accepted with conditions**.

The following conditions were documented:

- Annual SOC 2 Type II report submission
- Quarterly access review evidence
- Defined incident notification timelines
- Periodic reassessment aligned with the organization’s medium-risk review cadence

The risk acceptance decision was approved by the designated risk owner in accordance with the organization’s risk appetite and governance model.

Ongoing Monitoring and Review

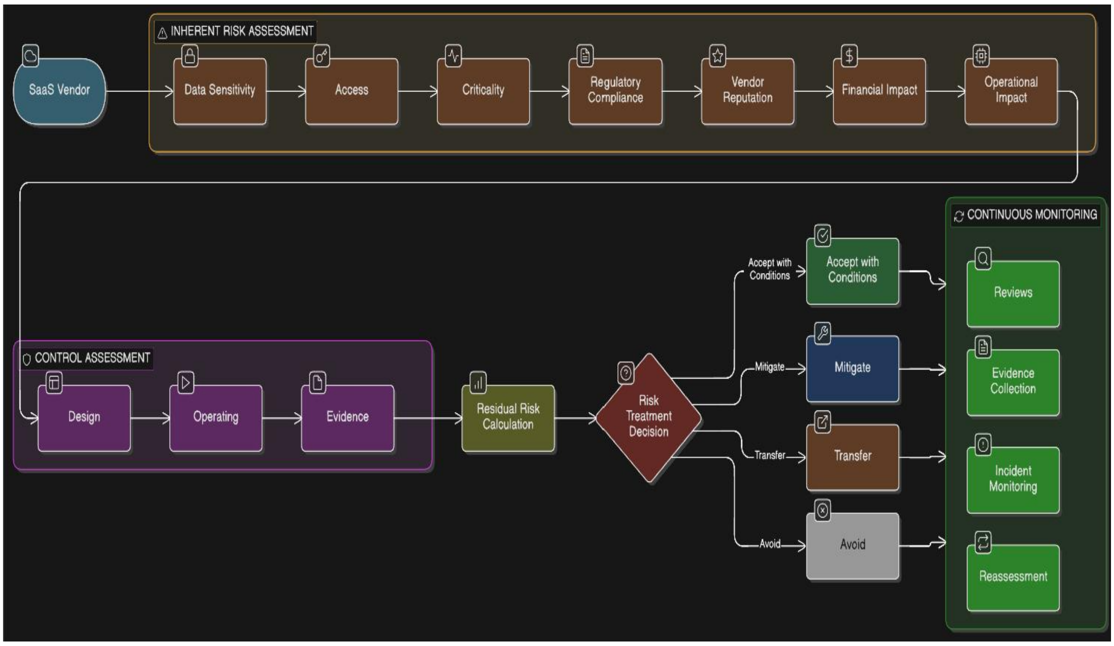
The vendor was onboarded into the continuous monitoring program. Risk reviews are scheduled periodically, and any significant changes in data scope, access level, or security incidents trigger an immediate reassessment.

This case study demonstrates the practical application of the GRC framework, showcasing how inherent risk, control effectiveness, and business context are balanced to support informed, risk-based decision-making.

SOC 2 Type II Evidence Review (Vendor: Cloud CRM)

Control Area	SOC 2 Auditor Observation	Framework Alignment	Validation Status
Data Encryption	Verified AES-256 for data at rest; TLS 1.2+ for data in transit.	Domain 3: Data Protection	**PASS**
Access Control	Tested 25 new hires; 100% had MFA enabled and signed NDAs.	Domain 2: IAM	**PASS**
Availability	Auditor verified 99.9% uptime over the 6-month period.	Domain 4: Business Continuity	**PASS**
Incident Response	2/10 sample alerts had a 4-hour notification lag (Minor Gap).	Domain 5: Incident Response	**OBSERVATION**

Vendor Risk Assessment Process Flow



Deliverable 3

Automated Vendor Risk Register & Executive Dashboard

1. Overview

Deliverable 3 represents the **operational implementation** of the Enterprise Third-Party Vendor Risk Assessment Framework defined in Deliverable 1.

While Deliverable 1 establishes the governance model, risk methodology, and decision principles, Deliverable 3 translates those principles into a **working, executable risk management system**.

The deliverable is implemented as a **Microsoft Excel–based Automated Risk Register**, supported by formula-driven risk logic and an executive-level dashboard.

Its primary purpose is to ensure that third-party risks are:

- Assessed consistently
- Governed transparently
- Actioned within defined timelines
- Reported effectively to management

2. Role Within the Overall GRC Framework

The Automated Risk Register functions as the **single operational source of truth** for third-party risk management.

It operationalizes the following components of the framework:

- Vendor risk assessment methodology
- Inherent and residual risk calculations
- Control effectiveness evaluation
- Risk ownership and accountability
- Review cadence and escalation
- Executive reporting and oversight

This ensures that vendor risk management moves beyond policy documentation into **day-to-day risk governance and decision-making**.

3. Implementation Approach

The risk register is implemented using **Microsoft Excel**, selected to balance:

- Ease of adoption
- Transparency of logic
- Flexibility
- Audit traceability

Despite its spreadsheet-based implementation, the register is designed using **enterprise GRC design principles** and mirrors the structure of commercial Third-Party Risk Management (TPRM) platforms.

Automated formulas are used extensively to:

- Calculate risk score
- Assign risk ratings
- Determine review deadlines
- Flag overdue items

This reduces manual intervention and ensures consistent application of risk rules.

4. Structure of the Automated Risk Register

The register is structured to capture both **risk analytics** and **governance metadata**, enabling informed decision-making and audit defensibility.

4.1 Vendor & Risk Identification

Each record includes:

- Vendor Name
- Vendor Category (e.g., Cloud Provider, Payment Processor, SaaS)
- Risk Domain
- Risk Statement

This ensures clarity and consistency in how risks are documented and evaluated.

4.2 Inherent Risk Assessment

Inherent risk is calculated using a **factor-based scoring model**, considering parameters such as:

- Data sensitivity
- Level of system access
- Business criticality
- Regulatory and compliance exposure

This structured approach minimizes subjectivity and allows meaningful comparison of risk across vendors.

4.3 Control Effectiveness Evaluation

Control effectiveness is assessed using a **two-dimensional model**, aligned with audit and assurance practices:

Design Effectiveness: Whether the control is appropriately designed to mitigate the identified risk

Operating Effectiveness: Whether the control is functioning as intended in practice

The final control effectiveness score is derived as the average of these two dimensions, ensuring a balanced and defensible evaluation.

4.4 Residual Risk Calculation

Residual risk is calculated automatically by combining:

- Inherent risk score
- Control effectiveness score

Based on defined risk thresholds, residual risk is categorized into:

- Low
- Medium
- High
- Critical

This enables consistent and pre-approved risk decisions aligned with organizational risk appetite.

5. Risk Ownership & Accountability

To embed governance into daily operations, each risk record explicitly assigns:

Risk Owner – Accountable for the risk

Business Owner – Responsible for remediation activities

Approver – Authorized decision-maker for risk acceptance or escalation

This ensures clear accountability and aligns with RACI principles defined in the framework.

6. Risk Treatment, Review & Escalation

For each identified risk, the register captures:

- Risk treatment decision (Mitigate, Accept, Transfer, Avoid)
- Required remediation actions
- Target completion dates

The register includes:

- Defined review SLAs
- Automated due dates
- Overdue indicators

High-risk and overdue items are clearly identifiable, enabling timely escalation to management and the Risk Committee.

7. Evidence Management & Audit Readiness

The register incorporates evidence management to support audit and compliance requirements, including:

- Evidence references (policies, certifications, reports)
- Compliance indicators (e.g., ISO 27001, SOC 2)
- Audit readiness status

This design ensures continuous preparedness for:

- Internal audits
- External assessments
- Regulatory inquiries

8. Executive Dashboard & Management Reporting

An executive dashboard is layered on top of the risk register to provide senior management with a **concise, decision-focused view** of third-party risk posture.

The dashboard highlights:

- Distribution of vendor risk levels
- High-risk and critical vendors
- Overdue risk reviews
- Remediation status and trends
- Audit readiness indicators

The dashboard is designed for consumption by:

- CISO
- Risk Committee
- Senior Management

9. Tooling Alignment & Scalability

Although implemented in Microsoft Excel, the Automated Risk Register is designed to integrate seamlessly with the Microsoft ecosystem, including:

Power BI for advanced analytics and dashboards

SharePoint for centralized evidence storage

Power Automate for workflow automation and alerts

This enables a scalable transition from a spreadsheet-based implementation to a fully integrated GRC tooling environment without changes to the underlying risk methodology.

10. Value Delivered

Deliverable 3 transforms the Third-Party Vendor Risk Framework from a **static governance document** into a **living operating model**.

It enables the organization to:

- Operationalize third-party risk management
- Enforce accountability
- Support executive decision-making
- Maintain audit defensibility
- Scale vendor risk management as the organization grows

DELIVERABLE 4

RISK ACCEPTANCE MEMO

1. Purpose of the Risk Acceptance Memo

The Risk Acceptance Memo is a formal governance document used to record and approve decisions where residual vendor risk is knowingly accepted by the organization.

This memo ensures that:

- Risk acceptance is **intentional and documented**
- Accountability is assigned at the appropriate management level
- Decisions are **auditable and defensible**
- Accepted risks are subject to **time-bound review**

Risk acceptance does **not** eliminate risk. It acknowledges that residual risk remains after reasonable controls are applied and that the business has chosen to proceed based on informed judgment.

2. When a Risk Acceptance Memo Is Required

A Risk Acceptance Memo is required when one or more of the following conditions apply:

- Residual risk remains **medium or high** after assessment
- Required controls cannot be fully implemented within acceptable timelines
- Business dependency on the vendor outweighs the remaining risk
- Vendor limitations prevent full compliance with security or regulatory expectations
- Temporary risk waivers are requested

Low-risk vendors typically do not require a formal memo unless explicitly requested by governance bodies.

3. Risk Acceptance Memo – Standard Template

You can copy this **exact template** into your report or use it as a standalone document.

Risk Acceptance Memo

Vendor Name: ________________________
Service Description: __________________
Business Owner: _____________________
Risk Owner: __________________________

Assessment Date: _____________________
Residual Risk Level: ☐ Low ☐ Medium ☐ High

3.1 Description of the Risk

Provide a clear and concise description of the identified risk, including the potential business impact.

Example:
Unauthorized access to customer data hosted by the vendor could result in regulatory penalties, reputational damage, and loss of customer trust.

3.2 Summary of Assessment Findings

Summarize key findings from the vendor risk assessment, including major control gaps and contributing factors.

Example:

- ✓ Vendor lacks full encryption key ownership controls
- ✓ Incident response procedures exist but are not tested annually
- ✓ Compensating controls reduce likelihood but do not eliminate risk

3.3 Business Justification for Risk Acceptance

Explain why the organization is choosing to accept the residual risk.

Considerations may include:

- Criticality of the vendor to business operations
- Lack of viable alternative vendors
- Disproportionate cost or complexity of further mitigation
- Temporary nature of the identified risk

Example:
The vendor provides a mission-critical service with no suitable alternative in the short term. Additional mitigation measures are planned, but business operations require continued use of the service.

3.4 Risk Acceptance Decision

Based on the assessment and business justification, the residual risk associated with this vendor is formally accepted.

Acceptance Type:
☐ Permanent
☐ Temporary (Review required)

Acceptance Valid Until: ____________________

3.5 Conditions and Compensating Controls (If Applicable)

List any conditions associated with the risk acceptance.

Examples:

Increased monitoring frequency

Contractual commitments for future control improvements

Additional internal safeguards

3.6 Approval Authority

This risk acceptance decision has been reviewed and approved in accordance with the organization’s governance framework.

Role	Name	Signature	Date
Business Owner			
Risk Owner			
CISO / Risk Committee Representative			

4. Governance and Review Requirements

Risk acceptance must be reviewed upon:

- ✓ Expiration of the acceptance period
- ✓ Material change in vendor services or risk profile
- ✓ Security incident involving the vendor

Accepted risks remain subject to:

- ✓ Periodic monitoring
- ✓ Management reporting
- ✓ Audit and regulatory review

Failure to review accepted risks within defined timelines may result in escalation to the Risk Committee.

Fourth-Party Mapping

To support Nth-party visibility, each vendor entry includes:

- **Critical Fourth-Party Provider**: Identification of the primary infrastructure or service provider the vendor relies upon (e.g., AWS, Microsoft, Stripe).
- **Dependency Level**: Qualitative assessment of how critical the fourth-party is to the vendor's service availability

5. Value of the Risk Acceptance Memo

This memo strengthens vendor risk governance by:

- ◆ Making risk decisions **explicit rather than implicit**
- ◆ Assigning clear ownership and accountability
- ◆ Supporting transparent communication with leadership
- ◆ Demonstrating due diligence to auditors and regulators