**VENDOR DUE DILIGENCE WORKFLOW**

**Assessing and Managing Third-Party Risk for Security, Compliance, and Business Continuity**

This document outlines a comprehensive Vendor Due Diligence Workflow designed to help organizations evaluate, score, and continuously monitor third-party vendors for cybersecurity, privacy, and compliance risk. It provides a structured framework that aligns with leading standards such as ISO/IEC 27001, SOC 2, NIST SP 800-53, HIPAA, and GDPR.

Key components include:

* A business scenario with clear security and compliance objectives
* A step-by-step implementation guide with defined roles and deliverables
* A standardized vendor evaluation questionnaire
* A quantitative scoring model and risk tier matrix
* Control mappings to major frameworks and common risk domains
* Evidence collection strategies and tooling recommendations
* Ongoing monitoring and governance practices for sustained oversight

This workflow enables security, GRC, and procurement teams to make informed onboarding decisions, improve third-party accountability, and ensure audit readiness in fast-paced, regulated environments—especially in **SaaS**, **FinTech**, **HealthTech**, and **cloud-native** organizations.

**TABLE OF CONTENTS:**

[Business Scenario & Objectives: 2](#_Toc197266306)

[Implementation of Objectives: 2](#_Toc197266307)

[Vendor Evaluation Questionnaire 4](#_Toc197266308)

[Scoring Model 5](#_Toc197266309)

[Risk Categorization Matrix 5](#_Toc197266310)

[Control Mappings & Risk Themes 6](#_Toc197266311)

[Evidence Strategies & Tools 6](#_Toc197266312)

[Recommended Platforms: 6](#_Toc197266313)

[Monitoring, Reviews, and Governance 7](#_Toc197266314)

Business Scenario & Objectives:  
A startup or mid-sized business is scaling operations and outsourcing key functions (e.g., cloud hosting, payroll, marketing automation). As vendors gain access to customer data or core infrastructure, **security, privacy, and compliance risks** must be assessed and managed.

* **Objective 1**: Identify, assess, and document vendor risks prior to onboarding
* **Objective 2**: Ensure compliance with frameworks (e.g., SOC 2, ISO 27001, GDPR, HIPAA)
* **Objective 3**: Protect customer and company data from third-party risk exposure
* **Objective 4**: Maintain an auditable record of due diligence and vendor accountability

## Implementation of Objectives:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Step** | **Action** | **Responsible Party** | **Inputs** | **Outputs** | **Tools / Notes** |
| **1. Intake Request** | Business unit submits vendor request for approval | Business Unit (Procurement / Legal / Security Requestor) | Vendor name, description, data types, integration details | New vendor intake form | Intake form or ticketing system (e.g., Jira, ServiceNow) |
| **2. Initial Risk Tiering** | Security or Compliance team performs a quick risk triage | Security / GRC | Intake form, data classification | Preliminary risk rating (Low/Med/High/Critical) | Risk matrix aligned with sensitivity of data and system access |
| **3. Questionnaire Delivery** | Send vendor due diligence questionnaire | Security / Compliance | Vendor contact info, risk tier | Questionnaire sent | Secure form (e.g., OneTrust, Whistic, Google Forms) |
| **4. Documentation Request** | Request supporting documentation based on risk tier | Security / GRC | Compliance requirements, vendor tier | List of requested documents | Document checklist includes SOC 2, ISO certs, DPA, policies, etc. |
| **5. Vendor Response Review** | Evaluate questionnaire answers and verify documents | Security / Compliance Analyst | Completed questionnaire, documents | Response validation notes, flags | Manual review or automated scoring if using a TPRM platform |
| **6. Vendor Scoring** | Apply scoring model across all domains | Security / GRC | Review notes, evidence | Numerical risk score (0–100) | Weighted scoring matrix (see section 4) |
| **7. Risk Categorization** | Categorize vendor as Low, Medium, High, or Critical | Security / GRC | Final score, data sensitivity | Final risk classification | Refer to Risk Categorization Matrix (see section 5) |
| **8. Review & Approval** | Cross-functional review for decision and mitigation plan | Security + Legal + Business Unit | Risk classification, open issues | Vendor approval, conditional approval, or rejection | Record decisions in vendor register and email confirmation |
| **9. Contract Controls** | Incorporate security/privacy clauses into vendor agreement | Legal / Procurement | Final risk score, open gaps | Finalized contract with DPA, SLA, breach notification terms | Add-ons: NDA, cybersecurity insurance, right-to-audit |
| **10. Evidence Archival** | Store responses and documents for audit purposes | GRC / Compliance | Final documents, scorecard | Archived package with versioning | Store securely (e.g., SharePoint, Confluence, GRC platform) |
| **11. Onboarding & Access Control** | Implement vendor access restrictions and onboarding checklist | IT / Security | Approved vendor list | Role-based access, documented onboarding | Integrate with IAM, asset management, and ticketing |
| **12. Continuous Monitoring** | Reassess vendor risk periodically or upon change | GRC / Security | Expiry dates, vendor incidents | Updated risk tier, new documents | Frequency based on risk tier (annually, biannually, quarterly) |

**Process Triggers & Exceptions:**

* **Reassessment Triggers**:
  + New service offering
  + Breach or adverse event
  + Ownership or system changes
* **Exceptions Process**:
  + Escalate to Vendor Risk Committee if:
    - Vendor refuses due diligence
    - Critical vendor scores <50
    - Legal/Compliance has open concerns

## Vendor Evaluation Questionnaire

**Sections**:

1. **Organizational Security**
   * Do you maintain an Information Security Management System (ISMS)?
   * Are you ISO 27001 or SOC 2 certified?
2. **Access & Identity Management**
   * How is user access to customer data controlled and reviewed?
   * Do you support MFA and least privilege?
3. **Data Protection & Privacy**
   * Is data encrypted at rest and in transit?
   * Do you provide a Data Processing Agreement (DPA)?
4. **Compliance & Certifications**
   * List your compliance certifications (SOC 2, ISO, PCI, HIPAA).
   * Are you GDPR or CCPA compliant?
5. **Incident Management**
   * Do you have an incident response plan?
   * Average detection and response time?
6. **Business Continuity & Disaster Recovery**
   * Do you test BCP/DR plans annually?
   * Provide RTO and RPO values.
7. **Third-Party Risk Management**
   * How do you assess and monitor your own vendors?
8. **Security Testing & Monitoring**
   * Do you conduct regular vulnerability scans or pen tests?
   * What logging and alerting tools do you use?

## Scoring Model

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | **Weight (%)** | **Max Points** | **Scoring Criteria (0–4)** |
| Organizational Security | 15% | 15 | Policies, roles, certifications |
| Access Management | 10% | 10 | MFA, access reviews |
| Data Protection & Privacy | 20% | 20 | Encryption, DPA, retention |
| Compliance & Legal | 15% | 15 | Certification status |
| Incident Response | 10% | 10 | IR plan maturity |
| BCP / DR | 10% | 10 | Testing, RTO/RPO |
| Security Testing | 10% | 10 | Pentests, scan cadence |
| Third-Party Risk | 10% | 10 | TPRM documentation |

**Scoring Scale for Criteria (0-4)**:

* 0 = No evidence / poor response
* 1 = Partial / minimal controls
* 2 = Adequate with minor gaps
* 3 = Meets industry standards
* 4 = Exceeds best practices

## Risk Categorization Matrix

|  |  |  |
| --- | --- | --- |
| **Total Score** | **Risk Level** | **Recommended Action** |
| 90–100 | Low Risk | Approve; review annually |
| 70–89 | Medium Risk | Approve with mitigation plan & biannual review |
| 50–69 | High Risk | Conditional approval; must close gaps within 60 days |
| Below 50 | Critical | Do not engage; remediation required |

## Control Mappings & Risk Themes

|  |  |  |
| --- | --- | --- |
| **Risk Domain** | **Common Risks** | **Mapped Controls** |
| **Access Control** | Unauthorized data access | NIST SP 800-53: AC-2, ISO 27001: A.5, A.9 |
| **Data Protection** | Breach, misuse of data | ISO 27001: A.8, GDPR Art. 32, SOC 2 CC6.1 |
| **Vendor Oversight** | Cascading third-party risk | NIST SP 800-53: SR-5, ISO A.15, SOC 2 CC3.1 |
| **Incident Response** | Delayed notification, mishandling | NIST IR-4, ISO A.16, SOC 2 CC7.4 |
| **BCP/DR** | Downtime, loss of service | ISO A.17, NIST CP-2, SOC 2 CC7.1 |
| **Compliance** | Fines, legal exposure | ISO A.18, GDPR, CCPA, HIPAA |
| **Security Monitoring** | Blind spots, undetected breaches | NIST AU-6, ISO A.12, SOC 2 CC7.2 |

## Evidence Strategies & Tools

|  |  |  |
| --- | --- | --- |
| **Evidence Type** | **Example Tools** | **Audit Use** |
| **Security Reports** | SOC 2 Type II, ISO 27001 Cert, Pen Test Report | Validate control presence |
| **Policy Samples** | InfoSec, Access Control, IR Policy | Assess organizational maturity |
| **Configs / Screenshots** | MFA setup, logging config | Verify implementation |
| **Security Logs** | SIEM, EDR, DLP alerts | Prove monitoring effectiveness |
| **Diagrams** | Data Flow, Network Architecture | Map exposure and boundaries |
| **Legal Agreements** | DPA, SLA, subcontractor terms | Ensure legal coverage |

## Recommended Platforms:

* **GRC Tools**: OneTrust, Whistic, Vanta, Tugboat Logic
* **Project Tracking**: Jira, Asana, Confluence
* **Evidence Repositories**: Google Drive, SharePoint (with DLP & RBAC)

## Monitoring, Reviews, and Governance

**Monitoring Frequency** (Based on Risk Tier):

* **Low Risk** – Annual review
* **Medium Risk** – Biannual review
* **High Risk** – Quarterly check-ins, update evidence
* **Critical Risk** – Not approved until remediated

**Trigger Events for Reassessment**:

* Vendor breach or adverse event
* Changes to vendor services, data handling, or system integration
* Certification expiration or legal issues

**Governance**:

* Led by Security, GRC, or Vendor Risk Committee
* Monthly/quarterly reporting to executive leadership
* Vendor Risk Register maintained with current tier, last review date, and remediation items