FRAMEWORK

Vendor Risk Assessment Framework

Tiering methodology, 35-question assessment questionnaire, scoring framework, contract requirements, ongoing monitoring, and offboarding procedures.

Published by
Compliance Enablers LLP

Last Updated
March 2026

Pages
~14 pages

Introduction

Organizations today rely on an extensive ecosystem of third-party vendors, suppliers, and service providers. While these relationships drive efficiency and innovation, they also introduce significant risk. A vendor's security breach becomes your breach. A vendor's compliance failure becomes your compliance failure. A vendor's operational disruption becomes your operational disruption.

Regulatory frameworks including ISO 27001, SOC 2, GDPR, NIST CSF, DORA, and PCI DSS all require organizations to manage third-party risk effectively. Beyond compliance, robust vendor risk management is essential for protecting your data, maintaining operational resilience, and preserving customer trust.

This framework provides a complete, practical approach to assessing and managing vendor risk throughout the vendor lifecycle — from initial onboarding through ongoing monitoring to offboarding.

1. Vendor Risk Tiering Methodology

Not all vendors pose the same level of risk. Applying the same assessment rigor to every vendor is neither practical nor necessary. A risk-based tiering approach ensures you focus resources where they matter most.

Tiering Criteria

Evaluate each vendor against the following criteria to determine their risk tier:

Criteria	Description	Scoring Guidance
Data access	Does the vendor access, process, or store your data? What type of data?	Critical/personal/financial data = higher tier
Data volume	How many records does the vendor handle?	Higher volumes = higher tier
System access	Does the vendor connect to your systems or network?	Direct integration/network access = higher tier
Business criticality	How critical is the vendor to your operations? Could you function without them?	Essential/irreplaceable = higher tier
Replaceability	How quickly could you transition to an alternative vendor?	Difficult to replace = higher tier
Regulatory exposure	Does the vendor's service fall under specific regulations (GDPR, HIPAA, PCI DSS)?	Regulated processing = higher tier
Financial exposure	What is the annual contract value and potential financial impact of failure?	Higher value/exposure = higher tier

Tier Definitions

Tier	Label	Criteria	Assessment Depth	Review Frequency
Tier 1	Critical	Processes sensitive/personal data AND is business-critical AND has direct system access	Full assessment, on-site/virtual audit, continuous monitoring	Annually + continuous monitoring
Tier 2	High	Processes some data OR is moderately business-critical OR has limited system access	Comprehensive questionnaire, documentation review	Annually
Tier 3	Medium	Limited data access, not business-critical, no system integration	Standard questionnaire	Every 2 years
Tier 4	Low	No data access, not business-critical, no system access (e.g., office supplies, cleaning)	Basic due diligence only	Every 3 years or upon renewal

Tier Assignment Process

1. Complete the tiering assessment for each new vendor during intake.
2. Assign the tier based on the highest-scoring criteria (i.e., if data access is Critical-tier but business criticality is Medium-tier, the vendor is Tier 1).
3. Document the tiering rationale.
4. Reassess the tier annually or when the relationship scope changes.

2. Vendor Intake and Onboarding Process

Pre-Engagement Phase

Before any contract is signed or data is shared:

1. **Business justification**: The requesting business unit submits a vendor intake form describing the business need, proposed vendor, scope of services, and data involved.
2. **Initial screening**: Perform a basic background check — company registration, financial stability (credit reports, news), regulatory actions, publicly reported breaches, and reputation.
3. **Tier assignment**: Apply the tiering methodology to determine the appropriate level of due diligence.
4. **Risk assessment**: Conduct the assessment appropriate to the vendor's tier (see Section 3).
5. **Contract review**: Ensure the contract includes required security, privacy, and compliance clauses (see Section 7).
6. **Approval**: Obtain approval from the appropriate authority (risk committee for Tier 1, department head for Tier 2-3, procurement for Tier 4).

Onboarding Phase

Once approved:

1. **Access provisioning**: Grant only the minimum necessary access (least privilege). Document all access granted.
2. **Data sharing agreements**: Execute Data Processing Agreements (DPAs) where GDPR applies, and other required data sharing agreements.
3. **Security requirements communication**: Share your security policies and requirements with the vendor. Confirm their acknowledgment.
4. **Add to vendor register**: Record the vendor in the centralized vendor register with tier, risk score, contract details, renewal dates, and responsible owner.
5. **Set monitoring schedule**: Configure ongoing monitoring based on tier.

3. Assessment Questionnaire Categories

The depth of assessment varies by tier, but all assessments draw from the same question categories.

Category 1: Information Security

Assesses the vendor's security posture, controls, and incident management capability.

- Security governance structure and accountability.
- Security certifications and attestations (ISO 27001, SOC 2 Type II, CSA STAR).
- Access control policies (MFA, least privilege, role-based access).
- Encryption standards (in transit, at rest, key management).
- Vulnerability management and patching cadence.
- Penetration testing frequency and remediation practices.
- Security monitoring and incident detection capabilities.
- Incident response plan and breach notification procedures.

Category 2: Business Continuity & Disaster Recovery

Assesses the vendor's ability to maintain or restore services during disruptions.

- Business continuity plan (BCP) existence and testing frequency.
- Disaster recovery plan (DRP) with documented RTO and RPO targets.
- Geographic redundancy and failover capabilities.
- Backup procedures and restoration testing.
- Communication plan during disruptions.
- Historical incident record (outages, disruptions).

Category 3: Privacy & Data Protection

Assesses compliance with data protection regulations and privacy practices.

- Privacy policy and data protection officer (DPO) appointment.
- GDPR compliance posture (for EU data processing).
- Data processing agreements and sub-processor management.
- Data subject rights handling procedures.
- Data retention and deletion practices.
- Cross-border data transfer mechanisms.
- Privacy impact assessments for new processing activities.

Category 4: Financial Stability

Assesses the vendor's financial health and viability as a long-term partner.

- Financial statements (revenue, profitability, cash flow).
- Credit ratings and financial health indicators.
- Funding status and investor backing (for startups).
- Customer concentration risk.
- Insurance coverage (cyber liability, professional indemnity, general liability).

Category 5: Regulatory Compliance

Assesses the vendor's compliance with applicable laws and industry regulations.

- Relevant regulatory certifications (PCI DSS, HIPAA, FedRAMP, DORA).
- History of regulatory actions, fines, or sanctions.
- Compliance monitoring and audit programs.
- Anti-bribery and anti-corruption policies.
- Sanctions screening procedures.
- Whistleblower and ethics reporting mechanisms.

4. Risk Scoring Methodology

Scoring Framework

For each assessment question, assign a score:

Score	Rating	Description
1	Strong	Control is fully implemented, documented, tested, and operating effectively
2	Adequate	Control is implemented and documented but may have minor gaps
3	Needs Improvement	Control is partially implemented or has significant gaps
4	Weak	Control is minimal or largely ineffective
5	Non-Existent	Control does not exist

Category Weighting

Not all categories carry equal weight. Apply weights based on the relationship type:

Category	Weight (Data Processing Vendor)	Weight (Non-Data Vendor)
Information Security	35%	15%
Business Continuity	20%	25%
Privacy & Data Protection	25%	10%
Financial Stability	10%	25%
Regulatory Compliance	10%	25%

Calculating the Vendor Risk Score

1. Average the scores within each category.
2. Multiply each category average by its weight.
3. Sum the weighted scores to get the overall Vendor Risk Score.
4. Map to risk level:

Vendor Risk Score	Risk Level	Action
1.0 - 1.5	Low Risk	Approve; standard monitoring
1.6 - 2.5	Moderate Risk	Approve with conditions; enhanced monitoring
2.6 - 3.5	High Risk	Conditional approval; risk mitigation plan required; senior management approval
3.6 - 5.0	Critical Risk	Do not engage or require significant remediation before engagement; executive approval required

5. Due Diligence Requirements by Tier

Due Diligence Activity	Tier 1 (Critical)	Tier 2 (High)	Tier 3 (Medium)	Tier 4 (Low)
Full security questionnaire	Required	Required	Abbreviated	Not required
SOC 2 Type II / ISO 27001 review	Required	Required	Preferred	Not required
Penetration test report review	Required	Recommended	Not required	Not required
Financial health assessment	Required	Required	Basic check	Not required
Privacy / DPA review	Required (if data)	Required (if data)	Required (if data)	Not required
On-site / virtual audit	Required (biennial)	Optional	Not required	Not required
Reference checks	Required	Recommended	Optional	Not required
Insurance verification	Required	Required	Recommended	Not required
Background / sanctions screening	Required	Required	Basic	Not required
Sub-processor assessment	Required	Required	Recommended	Not required

6. Ongoing Monitoring

Assessment at onboarding is necessary but insufficient. Vendor risk changes over time.

Continuous Monitoring Activities

Activity	Description	Frequency	Applicable Tiers
Risk rating services	Subscribe to vendor risk rating platforms that provide continuous security scoring and alerts	Continuous	Tier 1, Tier 2
Financial monitoring	Monitor credit ratings, news, and financial filings for signs of distress	Quarterly	Tier 1, Tier 2
Breach monitoring	Track publicly reported breaches and security incidents involving your vendors	Continuous	All tiers
Compliance updates	Verify continued certification status (ISO 27001, SOC 2, PCI DSS)	Upon renewal	Tier 1, Tier 2, Tier 3
Performance monitoring	Track SLA adherence, uptime, incident frequency, and response times	Monthly	Tier 1, Tier 2
Reassessment	Conduct a full or abbreviated reassessment questionnaire	Per tier schedule	All tiers
News and regulatory scanning	Monitor for regulatory actions, lawsuits, or significant negative news	Continuous	Tier 1, Tier 2

Trigger-Based Reassessment

Reassess a vendor immediately when:

- The vendor reports a security breach.
- There is a significant change in the vendor's financial condition.
- The scope of the relationship changes (more data, more access, more criticality).
- Regulatory requirements change.
- The vendor undergoes a merger, acquisition, or change of ownership.
- Performance consistently falls below SLA thresholds.
- A vulnerability is discovered in the vendor's product or service.

7. Contract Requirements

Essential Security and Compliance Clauses

Every vendor contract (especially Tier 1 and Tier 2) should include:

1. **Security obligations**: Vendor must maintain security controls consistent with industry standards (reference ISO 27001, SOC 2, NIST CSF as appropriate). Specify minimum requirements (encryption, MFA, access controls, vulnerability management).
2. **Data processing terms**: For GDPR and other privacy laws, include a compliant Data Processing Agreement covering purpose limitation, data minimization, confidentiality, security measures, sub-processor management, data subject rights support, breach notification, data return and deletion, and audit rights.
3. **Breach notification**: Vendor must notify you of any security incident or data breach within a specified timeframe (e.g., 24 hours for Tier 1, 48 hours for Tier 2).
4. **Audit rights**: You (or your designated auditor) have the right to audit the vendor's compliance with contractual security and privacy obligations. Define frequency, scope, notice period, and cost allocation.
5. **Service Level Agreements (SLAs)**: Define availability targets, response times, resolution times, and penalties for non-compliance. Include incident severity classifications and escalation procedures.
6. **Sub-processor controls**: Vendor must obtain your approval before engaging sub-processors. Vendor remains responsible for sub-processor compliance. Maintain a list of approved sub-processors.
7. **Insurance requirements**: Vendor must maintain adequate insurance coverage, including cyber liability, professional indemnity, and general liability. Specify minimum coverage amounts based on risk tier.
8. **Business continuity obligations**: Vendor must maintain and test business continuity and disaster recovery plans. Provide evidence of testing upon request.
9. **Termination and exit provisions**: Define data return and deletion obligations upon termination. Specify transition assistance requirements and timelines. Include termination rights for material security breaches.
10. **Compliance with laws**: Vendor must comply with all applicable laws and regulations. Vendor must promptly notify you of any regulatory inquiry, audit, or action related to the services.

8. Vendor Offboarding

When a vendor relationship ends, manage the transition carefully to protect your data and security.

Offboarding Checklist

- [ ] **Notify the vendor formally**: Provide written notice of termination per contract terms.
- [ ] **Data return**: Request return of all your data in a usable format.
- [ ] **Data deletion**: Request and obtain written confirmation of deletion of all your data from the vendor's systems, including backups. Verify deletion where possible.
- [ ] **Access revocation**: Immediately revoke all vendor access to your systems, networks, and facilities. Disable vendor accounts, VPN access, API keys, and physical access badges.
- [ ] **Credential rotation**: Rotate any shared credentials, certificates, or API keys.
- [ ] **Knowledge transfer**: Ensure operational knowledge is transferred to replacement vendor or internal team.
- [ ] **Final invoice reconciliation**: Settle all outstanding payments and recover any prepaid amounts.

- [ ] **Remove from vendor register**: Update the vendor register to reflect terminated status and offboarding completion date.
- [ ] **Retain records**: Maintain assessment records, contracts, and correspondence for the required retention period (typically 3-7 years depending on regulatory requirements).
- [ ] **Post-mortem**: Document lessons learned for process improvement.

9. Sample Assessment Questionnaire

The following questionnaire provides 35 questions across all five assessment categories. Customize and expand based on your specific requirements and industry.

Information Security (Questions 1-10)

Q1. Does your organization hold a current ISO 27001 certification or SOC 2 Type II attestation? If yes, provide the certificate/report and its validity period.

Q2. Describe your information security governance structure. Who is ultimately accountable for information security, and what is their reporting line?

Q3. Do you enforce multi-factor authentication (MFA) for all access to systems that process or store our data? Describe your MFA implementation.

Q4. Describe your encryption practices for data in transit and at rest. Specify the algorithms and key lengths used.

Q5. How frequently do you conduct vulnerability assessments and penetration tests on systems within scope of our engagement? Provide the date and summary findings of the most recent test.

Q6. Describe your patch management process. What are your target timelines for applying critical, high, medium, and low-severity patches?

Q7. Do you have a documented incident response plan? When was it last tested? Provide a summary of the plan or the document itself.

Q8. Describe your access control model. How do you enforce the principle of least privilege? How frequently are access reviews conducted?

Q9. Do you have a Security Operations Center (SOC) or equivalent monitoring capability? Is it operated internally or by a managed service provider? What is the monitoring coverage (24/7/365)?

Q10. Describe your security awareness training program. How frequently is training delivered to employees? Do you conduct phishing simulations?

Business Continuity & Disaster Recovery (Questions 11-16)

Q11. Do you have a documented Business Continuity Plan (BCP)? When was it last tested? Provide a summary of the most recent test results.

Q12. What are your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the services you provide to us?

Q13. Describe your data backup procedures. How frequently are backups performed? Are backups tested for recoverability?

Q14. Do you have geographic redundancy for the infrastructure supporting our services? Describe your failover capabilities.

Q15. How will you communicate with us during a service disruption? Provide your escalation and communication plan.

Q16. Have you experienced any significant service disruptions in the past 24 months? If yes, describe the incident, duration, root cause, and remediation actions taken.

Privacy & Data Protection (Questions 17-23)

Q17. Do you have a designated Data Protection Officer (DPO) or equivalent privacy leader? Provide their name and contact information.

Q18. Where will our data be stored and processed? List all countries and data center locations. Are any sub-processors involved in processing our data?

Q19. Describe your data retention and deletion practices. How do you ensure data is securely deleted when no longer needed or upon contract termination?

Q20. How do you handle data subject access requests (DSARs) and other data subject rights requests related to our data?

Q21. Do you conduct Data Protection Impact Assessments (DPIAs) for new processing activities involving personal data?

Q22. What legal mechanism do you use for international data transfers (e.g., Standard Contractual Clauses, adequacy decisions, Binding Corporate Rules)?

Q23. List all sub-processors who will have access to our data. Describe your sub-processor due diligence and oversight process.

Financial Stability (Questions 24-28)

Q24. Provide your most recent audited financial statements or evidence of financial health (e.g., credit rating, annual report).

Q25. Do you carry cyber liability insurance? What are the coverage limits? Provide the certificate of insurance.

Q26. Do you carry professional indemnity (errors and omissions) insurance? What are the coverage limits?

Q27. What percentage of your total revenue does your largest single customer represent? (Assessing customer concentration risk.)

Q28. Have you experienced any material adverse changes in your financial condition in the past 12 months (e.g., significant losses, restructuring, change of ownership)?

Regulatory Compliance (Questions 29-35)

Q29. List all regulatory certifications and industry-specific compliance attestations your organization currently holds (e.g., PCI DSS, HIPAA, FedRAMP, DORA).

Q30. Have you been subject to any regulatory enforcement actions, fines, or sanctions in the past 5 years? If yes, provide details.

Q31. Do you have a formal compliance management program with assigned accountability and regular reviews?

Q32. Describe your anti-bribery and anti-corruption policies. Do you conduct sanctions screening for employees and business partners?

Q33. Do you have a code of conduct and ethics reporting mechanism (e.g., whistleblower hotline)?

Q34. How do you monitor changes in regulatory requirements relevant to the services you provide?

Q35. Are you willing to provide evidence of compliance upon request and to participate in audits as described in our contract terms?

10. Program Governance

Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	Overall accountability for vendor risk program; approval authority for Tier 1 vendors; risk acceptance authority
Vendor Risk Manager	Day-to-day program management; assessment coordination; monitoring; reporting
Procurement	Contract negotiation; commercial due diligence; vendor onboarding logistics
Legal	Contract review; DPA negotiation; regulatory compliance assessment
Business Owner	Vendor relationship management; performance monitoring; business justification
IT Security	Technical assessment; access provisioning and revocation; integration security review
Privacy / DPO	Privacy assessment; DPIA coordination; data processing agreement review

Reporting and Metrics

Report the following to leadership quarterly:

- Total vendor count by tier.
- Vendor assessments completed vs. due.
- Average vendor risk score by tier and trend.
- High-risk and critical-risk vendors and their remediation status.
- Overdue assessments and reassessments.
- Vendor incidents and breaches.
- New vendors onboarded and vendors offboarded.
- Contract renewals approaching with assessment status.

Conclusion

Third-party risk management is not optional — it is a business imperative and a regulatory requirement. The organizations that manage vendor risk most effectively are those that take a structured, risk-based approach: tier your vendors, assess proportionately, monitor continuously, enforce contractual obligations, and offboard cleanly.

This framework provides the structure you need to build or mature your vendor risk management program. Customize the questionnaire, adapt the tiering criteria to your industry, and invest in the tooling and processes that make vendor risk management sustainable at scale.

This resource is provided by Compliance Enablers — the unified GRC platform with 27 modules, 261+ compliance frameworks, and built-in security awareness training. Learn more at complianceenablers.com