Third-Party Risk Management (TPRM) Methodology

1. Vendor Intake

The intake process begins when a business owner requests a new third-party tool or service. The requester provides details on business purpose, data involved, required integrations, and operational impact. This stage determines whether the vendor enters the TPRM workflow.

2. Classification & Tiering

Vendor tiering determines the level of due diligence required. Tier 1 (High Risk) includes vendors handling production data or core operations. Tier 2 (Medium Risk) covers vendors with limited data access. Tier 3 (Low Risk) includes vendors with no sensitive data exposure.

3. Required Evidence by Tier

Evidence requirements increase with vendor tier. Tier 1 requires SOC 2 or ISO 27001, security questionnaire results, penetration testing summaries, and policy documentation. Tier 2 may require SOC 2 only, and Tier 3 may require minimal documentation.

4. Security Questionnaire

A structured 25-question security questionnaire is provided to assess access control, encryption, logging, incident response, business continuity, and privacy practices. Responses are validated against expectations for the vendor’s risk tier.

5. SOC 2 / ISO Review

SOC 2 Type II and ISO 27001 documentation is reviewed to understand control design and operating effectiveness. Key areas include change management, access provisioning, monitoring, vulnerability management, and incident response. Exceptions are documented and analyzed.

6. Control Testing & Gap Identification

Vendor controls are reviewed against internal expectations. Gaps are identified when controls are missing, incomplete, or not aligned with industry standards. Evidence quality and consistency are considered during this analysis.

7. Risk Scoring (Likelihood × Impact)

Each identified issue is rated based on likelihood and impact, generating a score between 1 and 25. Scores determine the overall vendor risk rating: Low, Medium, High, or Critical. High and Critical risks

require remediation before approval.

8. Remediation Process

Vendors are asked to provide remediation commitments for any High or Critical risks. Acceptable steps may include implementing MFA, enhancing logging, updating policies, or correcting permission issues. Timelines are reviewed for feasibility.

9. Approval Decision

Based on all collected evidence, the final decision is categorized as Approved, Conditionally Approved, or Not Approved. Conditional approval requires remediation steps completed within agreed-upon timelines.

10. Ongoing Monitoring

Approved vendors, especially Tier 1, undergo ongoing monitoring. This may include annual SOC 2 reviews, quarterly vulnerability updates, or periodic questionnaire refreshes to ensure controls remain effective.

11. Annual Review

Vendors handling sensitive data undergo an annual review. Evidence is refreshed, and risk scoring is updated based on new findings or changes to the vendor’s environment.

12. Offboarding

When a vendor is no longer needed, access is removed, data is deleted or returned per contractual requirements, and a formal offboarding review ensures closure of all obligations.