Third-Party Risk Management (TPRM) Workflow

1. Vendor Intake

The process begins when a business owner submits a vendor request. Key details include business purpose, data involved, required integrations, and operational impact.

2. Risk Tiering

Vendor is assigned a tier based on data sensitivity and operational importance. Tier determines the depth of due diligence required.

3. Evidence Collection

Based on the vendor tier, required documents such as SOC 2, ISO 27001, questionnaires, and policies are collected.

4. Security Questionnaire

Vendor completes a structured questionnaire assessing access control, encryption, monitoring, incident response, and privacy controls.

5. SOC 2 / ISO Review

Security team reviews SOC 2/ISO documentation for control maturity, exceptions, and alignment with internal requirements.

6. Risk Scoring

Findings are evaluated using the Likelihood × Impact model to determine risk levels: Low, Medium, High, or Critical.

7. Remediation

Vendors must address High or Critical risks. Action plans and timelines are documented and reviewed.

8. Approval Decision

Vendor is Approved, Conditionally Approved, or Not Approved based on evidence, scoring, and remediation commitments.

9. Ongoing Monitoring

Periodic monitoring activities ensure vendor controls remain effective. High-risk vendors receive closer oversight.

10. Offboarding

When vendor use ends, access is removed, data is handled per policy, and offboarding controls are confirmed.