Third-Party Risk Management (TPRM) – Step-by-Step Procedure

Company: DAS TECHNOLOGY SERVICES LLC
Author: Shaheer Nawaz, IT Support Specialist
Review Cycle: Annual
Version: V1.1
Approved By: IT Security Department
Owner: Information Security / Risk Management Team

---

1. Initiation s Vendor Identification

- **Trigger:** A department requests to board a new third party or renew an existing vendor.
- **Action:** Business owner submits a vendor intake/request form including service description, data access level, and integration details.

2. Risk Categorization

- **Input:** Vendor scope, data access type (e.g., PII, PCI, PHI), and system impact.
- **Action:** Assign vendor a risk level (Low, Medium, High) based on a risk matrix or scoring framework.
- **Tool(s):** BitSight, Security Scorecard, Process Unity, One Trust Vendor Risk Management and Prevalent.

---

3. Due Diligence s Security Assessment

- **Action:** For Medium to High-risk vendors:
  - Distribute and review security questionnaires.
  - Request relevant documentation (SOC 2, ISO 27001, Pen Test Reports, Data Flow Diagrams).
  - Conduct interviews or technical evaluations if needed.
- **Outcome:** Identify gaps or risks; assign a risk score or pass/fail status.

---

4. Contractual Security Requirements

- **Action:** Ensure contracts include:
    - Data protection clauses
    - Breach notification timelines
    - Access control expectations
    - Right to audit
- **Stakeholders:** Legal, Procurement, and InfoSec teams

---

5. Approval s Onboarding

- **Action:** Vendor is approved once risk is acceptable or mitigated.
- **Documentation:** Final security risk assessment report and signed contract stored in central repository (e.g., SharePoint, GRC tool).
- **System Access:** Provisioning is coordinated based on least privilege.

---

6. Ongoing Monitoring

- **Frequency:** Annually for high-risk vendors, biennially for medium, or as defined.
- **Actions:**
    - Review updated certifications (SOC 2, ISO, etc.)
    - Monitor for public incidents or breaches
    - Reassess if there is a major service or infrastructure change
- **Tools:** Manual reviews, automated vendor monitoring tools (if applicable)

---

7. Issue Management s Remediation

- **Trigger:** Identified gaps, incidents, or failed assessments.
- **Actions:**
    - Log issue in risk register

- Collaborate with vendor on remediation plan
- Track status and re-evaluate risk post-remediation

---

8. Offboarding

- **Trigger:** Vendor relationship ends or is terminated.
- **Actions:**
  - Revoke all access
  - Ensure return or deletion of data
  - Document offboarding checklist
- **Confirmation:** Business owner and IT to verify

G. Documentation s Audit Readiness

- **Action:** Maintain all records including:
  - Initial risk assessments
  - Contracts
  - Assessment responses
  - Monitoring activities
  - Issue logs

F. Risk Categorization

To determine the appropriate level of due diligence, contractual controls, and ongoing monitoring, DAS Technology Services, LLC classifies all third-party vendors based on the level of risk they pose to the organization.

Risk categorization is conducted using a combination of standardized tools, manual evaluation, and cross-functional review. This process includes:

- **Internal Risk Matrix**
  A structured framework that evaluates vendors across key dimensions such as:
    - Data sensitivity (e.g., PII, PHI, PCI)
    - Regulatory exposure
    - Operational criticality
    - Financial impact or dependency
- **Security Posture Assessments**
  Utilization of independent third-party platforms (e.g., Security Scorecard or equivalent) to assess and benchmark the vendor's security maturity and exposure to cyber threats.
- **Manual Scoring Criteria**
  Customized risk evaluation reviewed by DAS's **Compliance**, **Legal**, and **IT Security** teams, ensuring consistency and accuracy in the assessment process.

Each vendor is then assigned a formal **risk tier**—Low, Medium, or High—based on the cumulative score. This classification directly influences the scope, frequency, and depth of due diligence, contractual safeguards, and monitoring applied throughout the vendor lifecycle.