Global Retailer – Third-Party Risk Management Program

Project Type: Third-Party Risk Management (TPRM) Framework Design
Industry: Retail / E-commerce
Role: GRC / Cybersecurity Governance Practitioner
Duration: 5 weeks

---

1. Executive Summary

A global retail organization relied on dozens of third-party vendors for payments, logistics, cloud hosting, customer support, and in-store systems. Third-party risk activities were scattered across email, spreadsheets, and ad-hoc checks, with no unified view of vendor risk.

In this project, I designed a **practical, scalable Third-Party Risk Management (TPRM) program** that:

- Classified vendors by **criticality and data sensitivity**
- Introduced **structured due diligence questionnaires** mapped to PCI DSS, ISO 27001, SOC 2 and privacy expectations
- Established a **5-week implementation roadmap** from discovery through remediation tracking

The result was a clear, repeatable TPRM process that could be understood by security, procurement, and business stakeholders.

---

2. Context & Problem

The organization faced several challenges:

- No complete or reliable **vendor inventory**
- Vendors were approved based on **cost and functionality**, not risk
- Due diligence questions were inconsistent and driven by whoever requested the vendor
- Renewals and reassessments were not tracked, creating **blind spots** in risk exposure
- Leadership lacked a simple view of **“Which vendors worry us the most and why?”**

The objective of this project was to design a TPRM approach that could realistically be implemented by a small GRC team, while aligning with common frameworks and audit expectations.

---

3. Objectives

I defined four clear goals for the program:

1. **Visibility:** Create a single vendor inventory with ownership and basic risk attributes.
2. **Risk-based Tiers:** Classify vendors (e.g., Critical, High, Medium, Low) using simple, repeatable criteria.
3. **Standardized Due Diligence:** Introduce questionnaires and evidence requests aligned to key frameworks.
4. **Actionable Reporting:** Produce a basic risk register and dashboard summarizing key vendor risks and remediation status.

4. Approach & Methodology

4.1 Vendor Inventory & Data Collection

- Designed a vendor inventory template capturing:
    - Vendor name, service category, business owner
    - Data types processed (cardholder data, PII, internal data, etc.)
    - Hosting model (on-prem, SaaS, cloud provider)
    - Regions / jurisdictions (for privacy considerations)
- Populated the inventory from:
    - Sample contracts / invoices
    - Purchase records
    - “Shadow IT” sources such as marketing tools and SaaS apps

4.2 Vendor Tiering Model

Created a simple **scoring model** to tier vendors based on:

- **Data sensitivity** (e.g., payment data, PII, internal only)
- **Service criticality** (impact on revenue, operations, customer experience)
- **Connectivity** to core systems (direct network access vs. isolated)

Vendors were then assigned to tiers:

- **Tier 1 – Critical:** Payment processors, core cloud platforms, major logistics providers
- **Tier 2 – High:** Systems handling large volumes of PII or key operational functions
- **Tier 3 – Medium / Low:** Non-critical tools with minimal data exposure

Tiering determined how deep due diligence needed to be and how often to reassess each vendor.

4.3 Due Diligence Questionnaires

Developed **modular questionnaires** that could be reused across vendors:

- **Core Security & Governance Section**
    - Information security policies and governance
    - Access control, logging, incident response, business continuity
- **Compliance Section**
    - PCI DSS status for payment-related vendors
    - SOC 2 / ISO 27001 certification status
    - Data protection and privacy controls
- **Technical & Integration Section**
    - Network connectivity, encryption, interface security
    - Use of sub-processors / subcontractors

Questionnaires were mapped conceptually to frameworks (ISO 27001 controls, PCI DSS, SOC 2 trust principles) but written in business-friendly language.

4.4 Risk Evaluation & Register

For each vendor:

- Reviewed questionnaire responses and available certifications (e.g., SOC 2 report, ISO 27001 certificate).
- Identified **control gaps and weaknesses**, such as:
    - Missing MFA for administrative access
    - No documented incident notification process
    - Limited evidence of formal vulnerability management
- Logged risks in a **vendor risk register** with:
    - Risk description
    - Likelihood and impact rating
    - Overall risk level (e.g., Low/Medium/High)
    - Proposed treatment (accept, mitigate, transfer, avoid)
    - Action owner and target date.

4.5 Implementation Roadmap (5 Weeks)

Designed a practical **5-week rollout plan**:

- **Week 1 – Discover & Inventory**
    - Build initial vendor list, identify business owners
    - Apply first-pass tiering based on simple criteria
- **Week 2 – Design**
    - Finalize tiering model, questionnaires, and workflows
    - Agree on roles and responsibilities with security, procurement, and legal
- **Week 3 – Pilot**
    - Run the process on a small set of critical vendors
    - Refine questions and scoring based on feedback
- **Week 4 – Scale**
    - Roll out questionnaires to all Tier 1 and Tier 2 vendors
    - Populate the vendor risk register and start remediation discussions
- **Week 5 – Report & Improve**
    - Build summary dashboard (e.g., number of vendors by tier, top risks, remediation status)
    - Document lessons learned and suggested enhancements (automation, tooling, integration with procurement)

5. Deliverables

The engagement produced the following key artifacts:

1. **Vendor Inventory & Tiering Sheet**
   - List of vendors with assigned tier, data classification, and owner.
2. **TPRM Policy & Process Overview (High-Level)**
   - Scope, roles, and end-to-end process from onboarding to periodic review.
3. **Due Diligence Questionnaires**
   - Core security questionnaire
   - PCI DSS / payment-specific add-on
   - Cloud / SaaS-specific add-on.
4. **Vendor Risk Register Template**
   - Risk statements, rating logic, treatment options, and tracking fields.
5. **5-Week Implementation Roadmap & Summary Deck**
   - Visual timeline, responsibilities, and reporting views.

6. Outcomes & Impact

Key Outcomes:

- **100% visibility** into in-scope third parties in the new inventory
- **Prioritization** of effort: ~20% of vendors classified as Tier 1 & 2 but covering the majority of risk
- Clear understanding of **top vendor risks**, such as:
  - Lack of formal incident notification obligations in some contracts
  - No independent assurance (e.g., SOC 2 or ISO 27001) for certain critical SaaS tools
- A simple, repeatable process that could later be:
  - **Automated** in a GRC / TPRM tool
  - Integrated with procurement and renewal workflows
  - Extended to include continuous monitoring.

7. My Role & Contributions

In this engagement, I:

- Defined the **TPRM vision, scope, and objectives**
- Designed the **tiering model** and scoring logic
- Authored the **due diligence questionnaires** and mapped them conceptually to frameworks
- Built the **vendor inventory, risk register, and reporting layout**
- Designed the **5-week rollout plan** and documented roles & responsibilities
- Summarized the work in a one pager format suitable for stakeholders.

---

8. Lessons Learned & Next Steps

Key lessons from this project:

- TPRM programs succeed when they start **simple and practical**, then mature over time.
- Vendor tiering is essential—treating all vendors the same overwhelms both the business and security teams.
- Even without a dedicated TPRM tool, **structured spreadsheets + clear ownership** can significantly improve visibility and decision-making.