SCAN FOR THE TEMPLATE

JOB DESCRIPTION TEMPLATE

Third-Party Risk Manager

Owns the vendor and supplier risk program, from onboarding due diligence through ongoing monitoring and offboarding.

Department	Risk Management / Third-Party Risk / Procurement
Reports to	Chief Risk Officer / Head of Operational Risk / VP Procurement
Location	Remote / Hybrid / On-site
Employment type	Full-time
Experience	6 to 10 years

POSITION OVERVIEW

The Third-Party Risk Manager leads the organization's third-party and vendor risk management program. This role governs how the organization identifies, assesses, mitigates, and monitors risks introduced by suppliers, service providers, and other external relationships across their full lifecycle.

Partnering with procurement, information security, legal, compliance, and business owners, the Third-Party Risk Manager sets due diligence standards, drives ongoing monitoring, and manages concentration and fourth-party risk. The role keeps the organization protected as its reliance on outside providers grows.

This is a hands-on program leadership role for a risk professional who can balance rigor with the pace the business needs to onboard and manage vendors.

KEY RESPONSIBILITIES

THIRD-PARTY RISK PROGRAM

- Develop and maintain the Third-Party Risk Management (TPRM) framework and policy.
- Define risk tiering and due diligence requirements by vendor criticality.
- Maintain the third-party inventory and risk register.
- Report on program status and vendor risk posture to leadership.

DUE DILIGENCE AND ONBOARDING

Lead risk assessments across information security, privacy, financial, operational, regulatory, and reputational domains before contracts are signed. Evaluate:

- Information security and data protection controls
- Financial stability and business continuity
- Regulatory and compliance posture
- Concentration and fourth-party dependencies

ONGOING MONITORING

- Run periodic reassessments based on vendor tier and risk.
- Monitor performance, security ratings, and external risk signals.
- Track remediation of identified vendor issues to closure.
- Manage vendor risk exceptions and approvals.

CONTRACTS AND RISK PROVISIONS

Partner with legal and procurement to embed risk, security, privacy, and audit provisions into contracts. Confirm right-to-audit, breach notification, and service-level terms reflect the organization's risk appetite.

CONCENTRATION AND RESILIENCE

Assess concentration risk, single points of failure, and critical-vendor dependencies. Support business continuity and exit planning for material relationships.

OFFBOARDING

Manage the risk aspects of vendor exit, including data return or destruction, access removal, and closure of the relationship in the inventory.

REQUIRED QUALIFICATIONS

- Bachelor's degree in Business, Risk Management, Information Systems, Finance, or a related discipline.
- 6 to 10 years of experience in third-party risk, vendor management, operational risk, or information security.

- Strong knowledge of due diligence, risk assessment, and vendor lifecycle management.
- Familiarity with security, privacy, and regulatory requirements that apply to outsourced services.
- Experience operating a vendor risk platform or GRC tool.
- Ability to work across procurement, legal, security, and business stakeholders.

PREFERRED CERTIFICATIONS

One or more of: CTPRP, CRISC, CISA, CISSP, CIA, or equivalent risk certification.

TECHNICAL KNOWLEDGE

Third-party risk management, vendor due diligence, risk tiering, ongoing monitoring, contract risk review, concentration and fourth-party risk, business continuity, information security controls, and GRC and vendor risk platforms.

ESSENTIAL COMPETENCIES

Analytical judgment, stakeholder management, negotiation and influence, clear communication, program management, and the ability to balance risk rigor with business speed.

SUCCESS MEASURES: FIRST 12 MONTHS

- Refresh the TPRM framework, policy, and risk tiering model.
- Complete a full inventory of active third parties.
- Reassess all critical and high-risk vendors.
- Stand up an ongoing monitoring cadence by tier.
- Reduce the backlog of overdue vendor assessments.
- Strengthen risk provisions in the standard contract template.
- Establish concentration and fourth-party risk reporting.
- Deliver a leadership dashboard on vendor risk posture.