

Third-party risk management in practice can be a complex ecosystem of processes, tasks, timing and risk mitigation. Effective third-party risk management ensures that various responsibilities and requirements are distributed across a range of accountable stakeholders, each with a specific job to do.

Charts can help more easily sort it all out to show who does what at a high level. We've created some options that are ready to print or save to refer to as needed throughout your day-to-day work.



Regulators Governance Board of Directors Senior Leadership Risk Committees Oversight and

Lines of Business Management Vendor Owner

irst Line

Sourcing or Procurement

Third-Party Risk Management

Subject Matter Experts
Info Sec
Finance
Compliance
Business
Continuity

Internal Audit

Third Line

Oversight and Governance

- Regulators
- Board of Directors
- Senior Leadership
- Risk Committees

First Line

- Lines of Business
- Vendor Owner
- Vendor

Second Line

- Sourcing or Procurement
- Third-Party Risk Management
- Subject Matter Experts

Third Line

Internal Audit

Board of Directors

Responsibilities:

- Approves vendor management policies
- Sets the "tone-from-the-top"

 Remains involved in critical and high-risk vendor activities

Senior Leadership/The Executive Team

Responsibilities:

- Develops the process, procedures and projects
- Reviews the policy

- Assigns TPRM responsibilities
- Reviews SLA reporting to make informed decisions

Lines of Defense

First line of defense Lines of Business (Departments)	Second line of defense Dedicated Third-Party Risk Management Team/Third-Party Risk Manager/Third-Party Risk Management/Enterprise Risk/Compliance Department	
Vendor Owner/Product Owner	Responsibilities: Oversees vendor risk Escalates issues Identifies emerging risks and reports to senior leadership and the board	F
 Responsibilities: Manages the vendor relationship day-to-day Completes risk assessments Monitors and reports on vendor performance 		•
Vendors	SMEs .	
Responsibilities:Provides the product or service to your organization	Responsibilities: Provide formal assessments of the sufficiency of the vendor's controls and the severity of gaps or issues.	

issues

Third line of defense

Internal Audit/Oversight and Accountability

Responsibilities:

- Identifies program gaps or issues
- Shares best practices or advice on improvements

Responsibilities: Third line of defense Compliance Provide guidance on how organizations Internal Audit Responsibilities: need to comply with industry laws Responsibilities: Provides formal assessments · Identifies program gaps or issues on the vendor's compliance · Shares best practices or advice on gulators improvements InfoSec Responsibilities: Subject Matter Experts **Examiners** · Provides formal assessments Responsibilities: on the vendor's information Responsibilities: · Provide formal assessments of security controls Second line of defense · Ensures that the organization's TPRM D the sufficiency of the vendor's **Dedicated Third-Party Risk** program is compliant with industry controls and the severity of Management Team/Third-Party regulations gaps or issues **Business Continuity** Risk Manager/Third-Party Risk Management/Enterprise Responsibilities: Risk/Compliance Department Provides formal assessments on the vendor's BC/DR plans Responsibilities: Oversees vendor risk Escalates issues Responsibilities: · Identifies emerging risks and **Finance** Approves vendor management policies reports to senior leadership Responsibilities: Sets the "tone-from-the-top" and the board Provides formal assessments Remains involved in critical and highcto risk vendor activities on the vendor's finances ire Legal Responsibilities: First line of defense **Senior Leadership Lines of Defense** · Provides formal assessments Lines of Business (Departments) of on the vendor contract Responsibilities: Develops the process, procedures 5 and projects · Reviews the policy Vendor Owner Vendors 09 Assigns TPRM responsibilities · Reviews SLA reporting to make Responsibilities: Responsibilities: M Manages the vendor relationship day-to-day Provides the product or service to your informed decisions Completes risk assessments organization · Monitors and reports on vendor performance

