Who Is Responsible for Third-Party Risk Management?

Who Is Responsible for Third-Party Risk Management?

Third-party risk management (TPRM) is the practice and process of identifying and appropriately managing the risk present in your vendor relationships. It's meant to safeguard your organization and its customers from the risk of undesired events and impacts, such as data breaches, a sudden or loss of services, or in the case of regulated industries, fines and other enforcement actions that could negatively impact your revenue and reputation by outsourcing to vendors.

While it's a relatively simple concept, third-party risk management in practice is actually 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. Third-party risk management is a "team sport" and requires more than just one or two people to do the job right.

Let's explore the various roles and responsibilities that ensure effective third-party risk management.

Three Lines of Defense

Many industries utilize a third-party risk management model called Three Lines of Defense, Three Lines or even 3LOD. No matter what it's called, it's designed to give the executive team and the board clarity on which line is responsible for which areas, how each function and responsibility interconnects as well as which risks each function or activity should monitor.

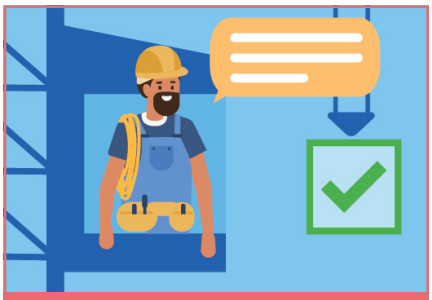
The Three Lines of Defense model splits responsibility for vendor risk into:

First Line

Responsible for the products or services provided by the vendor – identifies and manages risk

Second Line

Oversees vendor risks – the TPRM team, enterprise risk team and SMEs such as compliance, legal, finance and infosec are included in this line



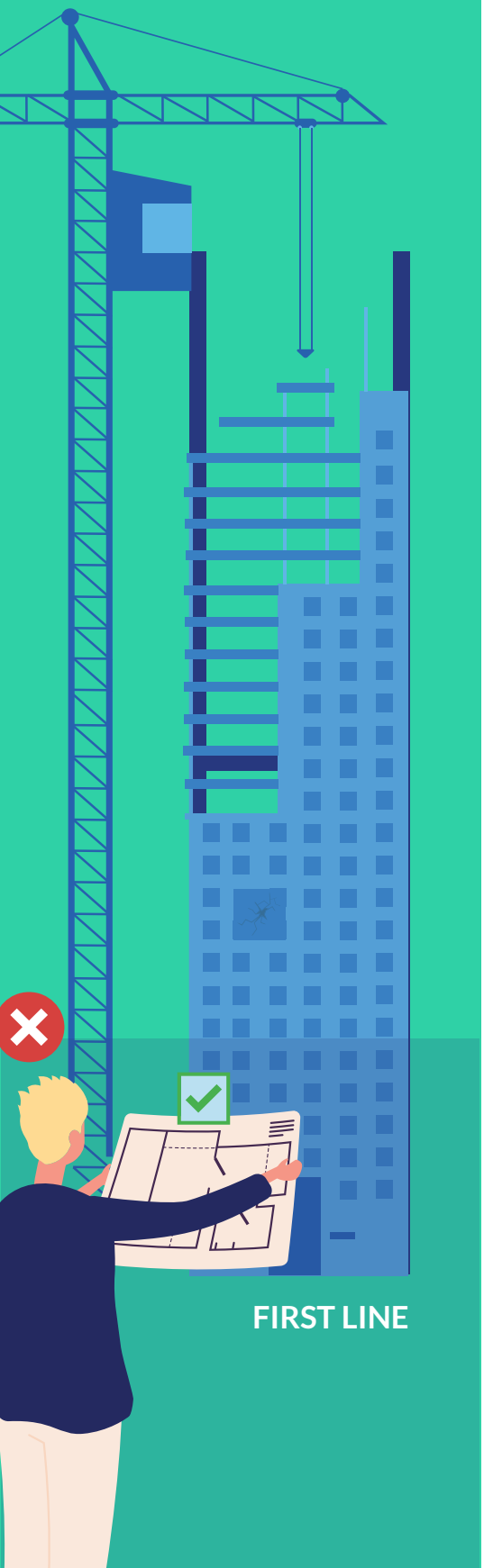
Third Line

Provides independent assurance over risks and monitors the effectiveness of risk management activities, such as internal audits

The Board/Executive Team

The board and executive team sit across these three lines. They determine the corporate vendor risk agenda, determine the vendor risk strategy and are responsible for oversight and governance.

Whether you adhere to the specific Three Lines Model is up to you and your organization; however, best practices highlight the individual roles and responsibilities listed in the following sections.



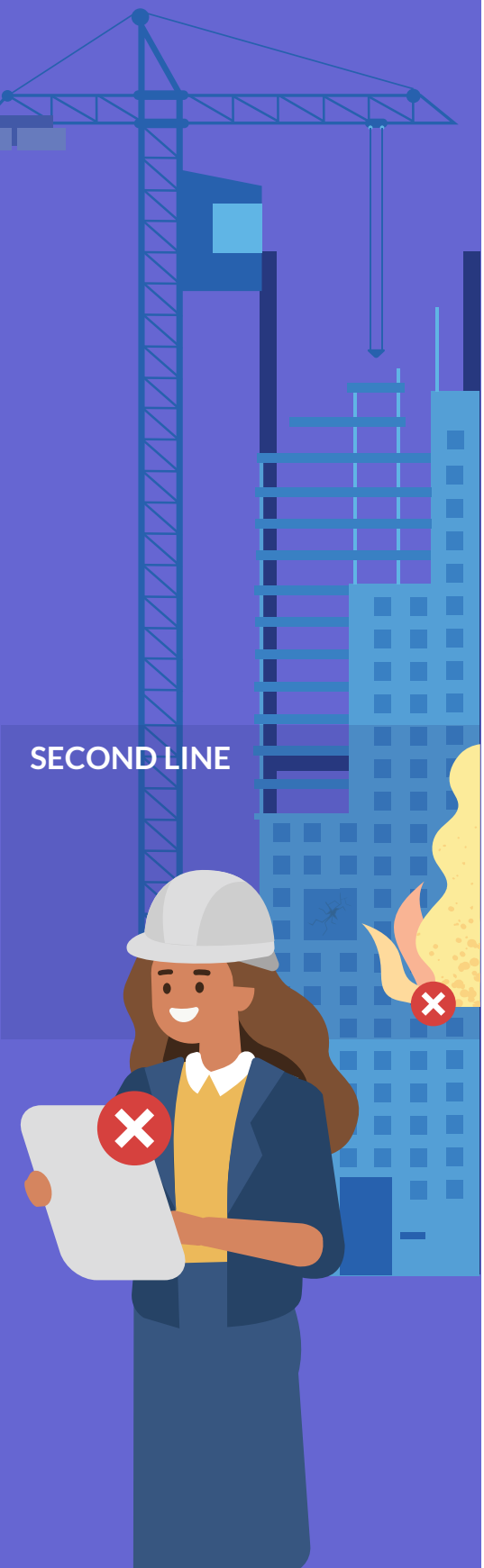
The First Line

Vendor Owner/Product Owner

These individuals are usually found in the line of business (department). They're the people responsible for the products or services provided by the vendor. They're also responsible for identifying and managing risk as part of their role in accomplishing their business objectives. This requires an understanding of organizational objectives and legal, regulatory and industry norms for the product or service provided.

The first line is responsible for the following:

- ☑ Determining the business requirements for the product or service to be provided
- ☑ Identifying suitable vendors to provide the product or service
- ☑ Identifying the risks inherent in the product and service (completion of an internal inherent risk assessment)
- ☑ Setting the right expectations for prospective vendors, including participation in all required due diligence, risk and participating in the negotiation of the vendor contract
- ☑ Setting appropriate service level agreements and key performance indicators with the vendor
- ☑ Managing and reporting vendor performance and addressing declining performance, if necessary
- ☑ Managing known vendor risks and identifying, reporting and managing new and emerging vendor risks or relating to the product or service industry
- ☑ Establishing and managing a vendor exit strategy



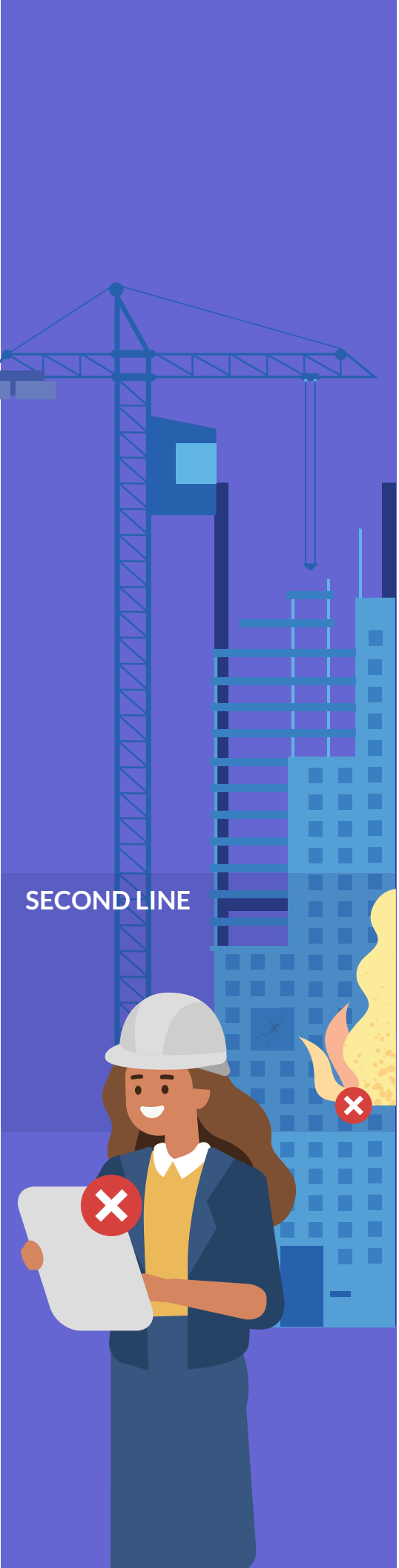
The Second Line

Dedicated Third-Party Risk Management Team/Third-Party Risk Manager/Third-Party Risk Management/Enterprise Risk/Compliance Department

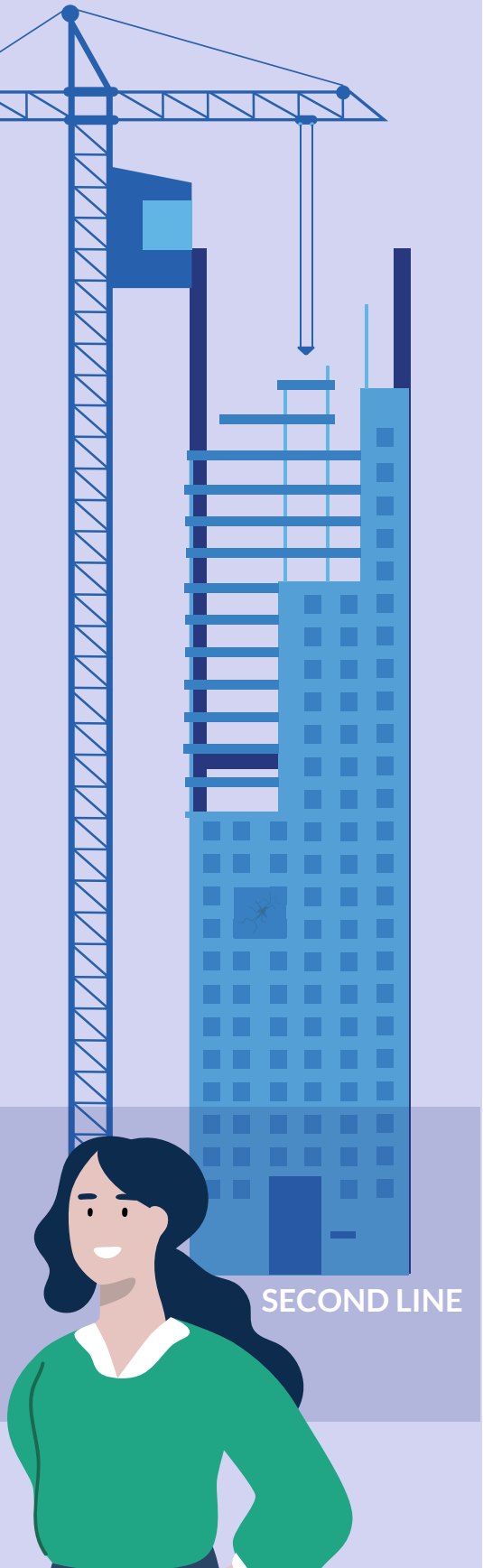
These teams provide the policies, frameworks, tools, techniques and support to enable vendor risk management and compliance in the first line. It monitors the first line third-party risk management activities to determine if risk measurement is consistent and effectively executed.

The second line is responsible for the following:

- ☑ Ownership of the third-party risk management governance documents (policy, program, procedures)
- ☑ Ownership and management of the third-party risk management framework, tools (including any third-party risk management software platform), processes and reporting
- ☑ Monitoring first-line vendor risk deliverables for accuracy, timeliness and quality
- ☑ Establishing and maintaining the methodology to assign vendor risk ratings
- ☑ Establishing and maintaining the criteria for critical vendors
- ☑ Establishing appropriate risk-based intervals for vendor risk and performance reviews
- ☑ Facilitating the third-party risk management lifecycle activities (onboarding, ongoing and offboarding)



- [x] Providing training or other educational support for the first line
- [x] Acting as the liaison between subject matter experts, vendor owners and vendors during initial due diligence and subsequent risk reviews
- [x] Advising and supporting the first line on vendor risk or performance issues
- [x] Creating and distributing third-party risk management reporting for committees, senior leadership and the board
- [x] Escalating vendor risk issues to senior leadership
- [x] Responding to an internal or external audit or regulatory requests and issues
- [x] Staying current on relevant regulatory and legal requirements and incorporating changes into the program
- [x] Self-monitoring and auditing the third-party risk management program



Subject Matter Experts (SMEs)

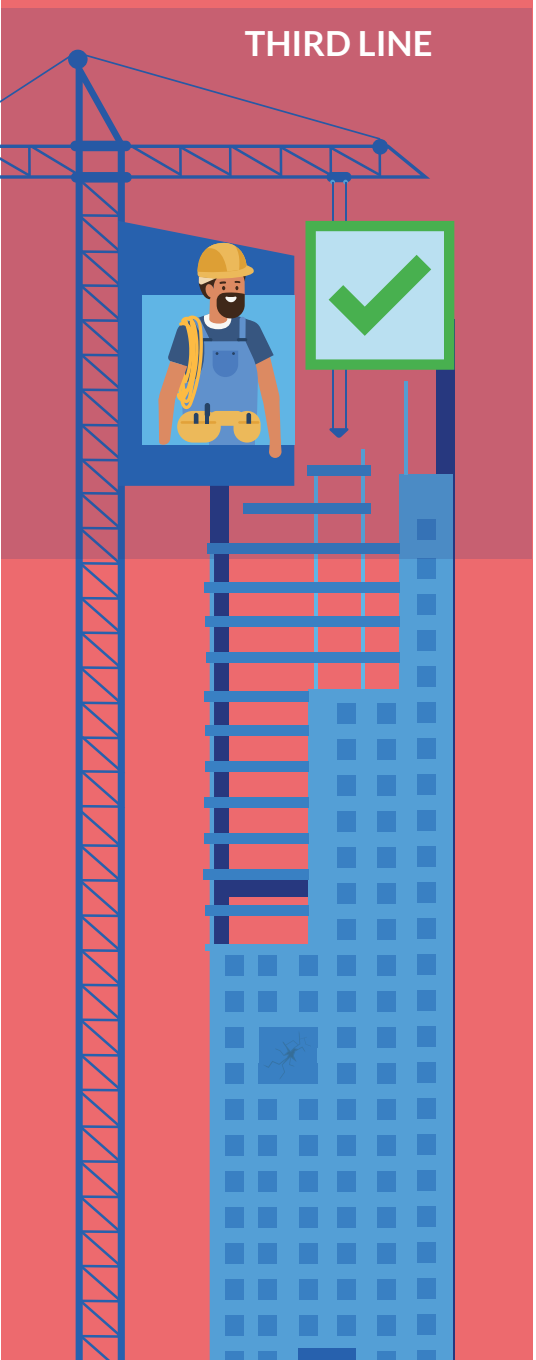
SMEs can be internal or external and are part of the second line

These are the individuals or organizations tasked with reviewing and assessing vendor controls through vendor due diligence and periodic risk reviews and providing a qualified opinion regarding the sufficiency of the vendor's controls.

They must have significant experience and knowledge to perform their role in third-party risk management. They essentially determine if the organization should do business with the vendor based on the strength of the vendor's control environment.

SMEs are responsible for the following:

- ☑ Reviewing vendor-provided documents and other materials to validate a substantial control environment
- ☑ Identifying any controls gaps or weaknesses
- ☑ Providing a documented assessment and recommendations related to the sufficiency of required vendor controls
- ☑ Determining if specific controls may be reasonably improved within a specific time frame
- ☑ Consulting with the first and second lines regarding the seriousness of any control deficiency
- ☑ If remediation is possible, reviewing additional documentation or evidence provided and delivering a second assessment to validate if the issue has been indeed remediated
- ☑ Staying current on appropriate laws, regulations, emerging risks and industry standards relevant to their risk domain



The Third Line

Internal Audit/Oversight and Accountability

The third line's primary role is to ensure that the first two lines operate effectively and in compliance with all rules, laws and regulations. The third line provides a qualified assessment of vendor risk governance, management and the effectiveness of internal third-party risk management controls to the organization's governing body and senior management. The third line can also assure regulators and external auditors that appropriate third-party risk management controls and processes are in place and operating effectively.

The third line is responsible for:

- ☑ Conducting regular audits on the third-party risk management program and on individual processes and controls within the program
- ☑ Ensuring that the vendor risk program is consistent with all applicable regulations and laws
- ☑ Identifying and documenting deficiencies within the third-party risk management program and monitoring the closure of the issues per the stated requirements
- ☑ Responding to regulatory or legal inquiries as appropriate
- ☑ Provide independent and unbiased evaluations of the third-party risk management policy, program, processes and work product
- ☑ Confirming to the executive leadership team and the board that identified gaps or weaknesses are remediated

External Oversight and Governance

Beyond the three lines of defense, there are additional oversight and governance roles and responsibilities. Let's dive into these:

Regulators

Regulators are the agencies appointed by the government to oversee and regulate specific domains or industries. A regulatory agency must serve and protect the public interest concerning the practice of a profession or industry. Regulatory agencies deal in administrative law, regulatory law, secondary legislation and rulemaking. They're also responsible for enforcing rules and regulations and supervising or overseeing those rules for the benefit of the public. They have powers to require that organizations or bureaus operating within a particular industry adhere to specific standards or deliver a set of outputs.

Examples of regulators:
Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC), Consumer Financial Protection Bureau (CFPB), Occupational Health and Safety Administration (OSHA) and the Federal Trade Commission (FTC). There are also state and local regulators (e.g., insurance is regulated at the state level).

Regulator responsibilities include the following:

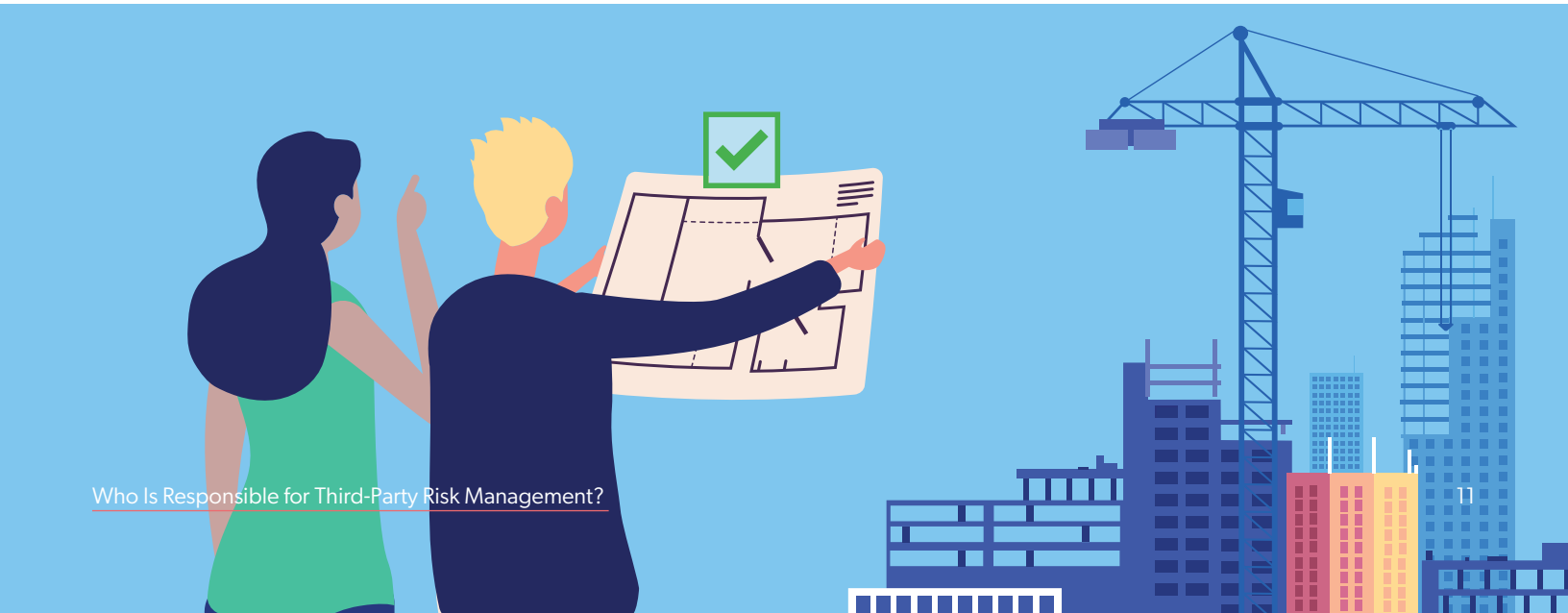
- ☑ Compelling transparency of information and decision-making on the part of the regulated organization
- ☑ Monitoring the performance and compliance of the regulated organization and publishing the findings of its investigations or audits
- ☑ Requiring that administrators give reasons explaining their actions and have followed principles that promote responsible decisions
- ☑ Carrying out enforcement actions, such as directing the organization to comply through orders, imposing fines or other financial penalties and/or revoking a license to operate
- ☑ Arranging review of administrative decisions by courts or other bodies

Examiners

Examiners are the representatives of the regulatory agency responsible for carrying out the official audits of an organization. Those audits or investigations are often called exams.

Examiner individuals or teams are responsible for the following:

- ☑ Monitoring and evaluating the organization's third-party risk management practices and their compliance with relevant regulations and laws
- ☑ Assessing management's ability to run the organization in a safe and sound manner
- ☑ Conducting fact-finding interviews with management and employees
- ☑ Reviewing and analyzing an organization's policies, procedures, governance documents and other records
- ☑ Reporting findings to their regulatory agency and usually to the board of directors and upper management of the examined organization
- ☑ Providing objective and non-judgmental analysis and evidence to support their findings
- ☑ Identifying and documenting severe violations of regulations and reporting them to appropriate levels of authority within their agency and the examined organization
- ☑ Recommending corrective action if warranted
- ☑ Assigning supervisory ratings to organizations and placing legal enforcement actions, civil money penalties or other punishments for non-compliance



Internal Oversight and Governance

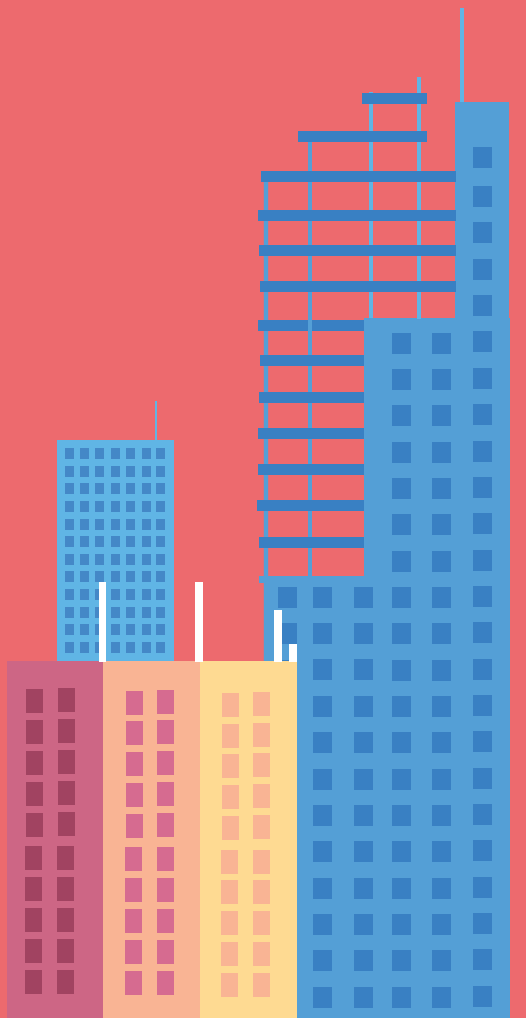
From a regulatory, legal and ethical business practices standpoint, the highest levels of the organization are ultimately accountable for the effectiveness of third-party risk management at the organizations. In fact, many regulators explicitly state their expectations for both the board and senior management.

Senior Management/The Executive Team

Senior management or the executive team are responsible and accountable for all third-party risk management practices and processes at their organization. Commonly these individuals don't participate in the day-to-day third-party risk management work activities. Still, they're ultimately accountable for ensuring those activities are appropriate for the risk level, that effective controls are in place and the corporate governance over third-party risk management is effective.

Senior management or the executive team are responsible for the following:

- ☑ Setting the "tone-from-the-top," ensuring that the importance of third-party risk management is understood through the organization
- ☑ Integrating consideration of vendor risk and third-party risk management into strategy development and business decision-making throughout the organization
- ☑ Ensuring that enough resources are allocated to third-party risk management, including skilled and competent individuals responsible for managing and overseeing vendor risk, and confirming they have the bandwidth to do so
- ☑ Providing other necessary resources such as subject matter experts, technology, tools or external consulting if warranted
- ☑ Reviewing and approving the third-party risk management policy
- ☑ Reviewing and understanding the types and level of risks present in the vendor portfolio
- ☑ Knowing which vendors are considered critical to the organization, how those vendors are performing, any open issues and the exit strategies and termination plans for those vendors
- ☑ Addressing vendor risk issues or concerns escalated to them in an effective and timely manner



The Board of Directors

Their involvement isn't just critical; it's a must. In fact, leading regulatory guidance mandates the board's involvement. It should be the executive leadership/board's responsibility to approve your third-party risk management policies and ensure that senior management sets the "tone-from-the-top."

The board (or executive leadership if there is no board) are responsible for the following:

- ☑ Emphasizing, via their oversight role, the CEO and senior executives must prioritize third-party risk management
- ☑ Integrating consideration of vendor risk and third-party risk management into strategy development and business decision-making throughout the organization
- ☑ Identifying and reviewing ongoing monitoring results of critical activities and vendors
- ☑ Reviewing the results of periodic independent reviews, both internal and external, of the organization's third-party risk management process
- ☑ Reviewing and advising levels of risk across the vendor portfolio
- ☑ Ensuring that senior management has allocated sufficient resources to ensure effective third-party risk management
- ☑ Approving risk-based policies that oversee the third-party risk management process

Third Parties aka Vendors

Of course, vendors also play a substantial role in third-party risk management. As the entities are actually responsible for the products and services in question, vendors have high accountability and responsibility for ensuring that their inherent risks are identified and managed appropriately.

Vendors are responsible for the following:

- ☑ Meeting all the required terms and conditions of their contract
- ☑ Formalizing and documenting their third-party risk management practices, processes and procedures
- ☑ Conducting risk-appropriate vendor due diligence, risk monitoring and performance monitoring of their vendors
- ☑ Training staff to be knowledgeable and compliant with all laws and regulations
- ☑ Establishing well-designed and tested business continuity and disaster recovery plans
- ☑ Participating in all due diligence and risk monitoring activities requested by their clients/customers
- ☑ Establishing and maintaining quality assurance and control procedures
- ☑ Complying with all laws and regulations
- ☑ Avoiding situations or practices that could harm them or their customers' reputations or brands
- ☑ Forbidding unethical business practices that violate human rights, civil rights or otherwise harm their employees or the public

In summary, there are many different roles and responsibilities within the practice of third-party risk management. Each role has distinct requirements to be met and unique skills required to accomplish the responsibilities.

To ensure that the roles work well together, it's essential to discuss and communicate the roles to those responsible and other stakeholders. Follow up by formalizing the details of who, what, why and when in your third-party risk governance documents. Then, you've got a team who can help your organization run a successful third-party risk management program.

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance and more.