WHAT/WHY/WHO/HOW of Vendor Risk Management

The WHAT

Defining Vendor Risk Management

Vendor risk management is the practice and process of identifying, assessing, managing, and monitoring the risks posed to an organization and its customers through its vendors. It involves securing the organization's operations against avoidable interruptions, controlling costs, driving service excellence, protecting your brand and reputation, and ensuring regulatory and legal compliance. It's also referred to as vendor management, third-party risk management, or supplier risk management.

The WHY

The Strategic Value of Vendor Risk Management

Vendor risk management aims to mitigate third-party risks associated with outsourcing a product or service and promote stronger vendor relationships.

Here are several reasons why vendor risk management is so important:

- It's a regulatory requirement for many industries
- It's a best practice
- It can yield strategic advantages
- It has a positive ROI
- It protects your organization by:
  - Enabling better vendor selection
  - Improving your organization's cybersecurity profile
  - Driving improved service and innovation
  - Confirming vendors perform as agreed
  - Reducing the potential for supply chain disruptions

A lack of vendor risk management results in operational issues, missed opportunities, and missed contract cancellations and renewals, ultimately costing your organization time, resources, and money. The overall strategic value of a vendor risk management program lies in its organization and optimization.

The WHO

The Parties Involved in Vendor Risk Management

Board of Directors
The board of directors sets the "tone-from-the-top" and is responsible for ensuring that senior management and the organization execute the vendor risk management program effectively. They also approve the vendor risk management policy and review the program's effectiveness regularly.

Senior Management
Senior management ensures that vendor risk management is a priority for the organization. They hold stakeholders accountable for fulfilling their roles and responsibilities, address concerns, review and approve the policy, and determine whether the risks in the vendor portfolio are acceptable. They're also responsible for ensuring adequate resources (money, technology and tools, and qualified staff) to execute vendor risk management effectively.

Vendor Risk Management Team
This individual or team is tasked with maintaining the vendor risk management framework, which includes all the processes, requirements, rules, and tools needed to effectively manage vendor risk. They must ensure that the vendor risk management policy, systems, workflows, documentation, and processes are executed properly. They're also responsible for issue management and reporting their findings.

Subject Matter Experts (SMEs)
Your organization must enlist the help of SMEs to conduct formal reviews and assessments. They provide qualified opinions on the vendor's risk management practices and controls, and they determine if the controls are sufficient to manage the identified risks. SMEs hold professional certifications or credentials in their specific risk domain.

Lines of Business
The lines of business identify and engage prospective third parties and manage those third parties in accordance with the vendor risk management program requirements.

Vendor Owner
Vendor owners are the individuals (usually within the line of business) responsible for managing the vendor relationship. They're tasked with completing all necessary vendor risk management activities, including inherent risk assessments, and ensuring the vendor returns all questionnaires and due diligence documents. They also negotiate contracts, monitor vendor risk and performance, and ensure that risks are effectively mitigated.

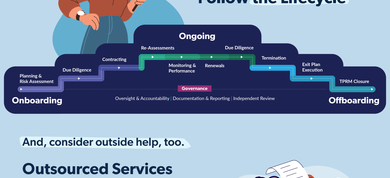
Third Party or Vendor
Your vendors provide products or services to your organization or to your customers on your behalf. They must follow your organization's vendor risk management requirements, meet contractual obligations and service level requirements, and provide high-quality products/services.

Internal Audit
Internal auditors review the vendor risk management program to ensure it meets regulatory requirements and best practices. They identify inconsistencies or gaps that must be addressed and report them to senior management and the board.

External Auditors and Examiners
External auditors or examiners monitor compliance with laws and regulations and assess policies, records, and governance documents. They also identify violations and recommend corrective action. Regulatory examiners represent a specific regulatory agency and conduct audits to verify compliance with regulatory requirements and guidelines within their jurisdiction. If there are issues, regulators can issue enforcement actions ranging from written warnings to penalties and fines to cease and desist orders.

Fourth or Nth Parties
Fourth or Nth parties are the business entities that work directly for your third parties. Even though your organization doesn't have a direct relationship with fourth or Nth parties, they may still directly or indirectly impact your organization or its customers.

The HOW



Follow the Lifecycle

And, consider outside help, too.

Outsourced Services

While you can't outsource vendor risks, you may consider outsourcing some vendor risk management activities. A qualified vendor risk management services provider can help ease heavy workloads by handling time-consuming tasks, such as collecting and reviewing due diligence.

By outsourcing portions of your vendor risk management program, you'll maximize your team's time and give them the bandwidth to focus on activities that identify and manage risk. Outsourcing to industry professionals and certified SMEs will also help fill any expertise gaps within your team.

Understanding vendor risk management's what, why, who, and how is the foundation for creating a comprehensive vendor risk management program.

Download sample assessments of vendor controls and see how Venminder can help reduce your third-party risk management workload.

DOWNLOAD NOW

PRINTABLE VERSION

venminder

Manage Vendors. Mitigate Risk. Reduce Workload.

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