WHAT IS THE PROCESS OF **VENDOR RISK MANAGEMENT?**

Vendor risk management is the process and ongoing practice of identifying, assessing, managing, and monitoring the risks posed to your organization and its customers through vendor relationships.

Vendor risk management is a best practice, and, for many organizations, it's also a regulatory requirement.

The process of vendor risk management requires the following:

Establish Governance and Oversight

The first step in the vendor risk management process is to determine your program's rules and requirements and memorialize them in your policy. However, to be able to do that, you must first do the following:

- Define roles and responsibilities. Who will be responsible for meeting the requirements?
- Establish the criteria for determining which vendors are critical to your organization. Then, develop and test the methodology to risk rate your vendors.
- Create inherent risk assessments to identify the types and amounts of risks in any engagement.
- Develop vendor risk questionnaires and document collection requirements.
- Establish the cadence for monitoring vendor risk and performance.

Determine Criticality

Determining if a product or service (and the vendor) will be critical to your operations is an essential activity. All vendors should be classified as critical or non-critical. These three questions can help you determine if a vendor is critical:

1 | Would a sudden loss of this third party cause significant disruption to our business?

2 | Would the sudden loss impact our customers?

3 | If the service is disrupted, would there be a negative impact on our operations if the time to restore service took more than 24 hours?

If you answered yes to any of these questions, you probably have a critical vendor.

Identify Inherent Risks

After you determine criticality, your inherent risk assessment will help you identify and assess all the types and amounts of risk possible in the engagement. When you compile results, you should have a risk rating such as low, moderate, or high risk. That risk rating informs the scope of your due diligence and it will help you establish the risk-based requirements and routines necessary to manage that vendor throughout the engagement.

Perform Initial Due Diligence

Once you determine the criticality and risk rating, determine your due diligence requirements and collect evidence of controls (i.e., documentation). Subject matter experts from each risk domain should review your vendor risk questionnaires and their documentation to determine if the respective controls are adequate. Once you have established that the controls are sufficient and that there are no open issues, you can negotiate the contract.

Negotiate the Contract

Your contract is one of your best vendor risk management tools. Ensure that your contract addresses documented service level agreements, information security and breach notification, compliance, business continuity, and disaster recovery requirements. Don't forget to include the all-important "right to audit" clause to ensure your access to vendor information when you need it.

Monitor Your Vendor

Once your vendor is up and running, it's essential not to drop the ball. Monitoring your vendor formally through periodic risk re-assessments and due diligence is a must. Establish appropriate risk review routines and stick to them. Keep on the lookout for new or emerging risks, and don't forget to monitor and manage vendor performance and schedule regular performance reviews. Vendor monitoring and oversight are important components in developing and maintaining productive and healthy vendor relationships.

Track Issues and Report Concerns

Issue management is an important element of effective vendor risk management. Whether the issue is discovered during the due diligence process or results from declining performance, it's important to document issues and track them until they are remediated. Most importantly, issues identified for critical vendors should be reported to senior management and the board.

The processes and practices of vendor risk management are essential to protect your organization and its customers against unnecessary risk.

By identifying, assessing, managing, monitoring, and analyzing vendor risk, effective vendor risk management processes support the development and maintenance of valuable vendor relationships.

Download free samples of Venminder's vendor Control Assessments and see how they empower third-party risk professionals in mitigating risks.

DOWNLOAD NOW

PRINTABLE VERSION

venminder

Manage Vendors. Mitigate Risk. Reduce Workload.

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