Mini Vendor Risk Assessment

GUIDEBOOK & BEST PRACTICES

venminder

What Is a Vendor Risk Assessment?

A vendor risk assessment examines and analyzes the risks posed to your organization or its customers through your vendor relationship. One purpose of a vendor risk assessment is to confirm that the vendor is a legitimate business with a solid reputation and to gather specific details regarding its controls and practices. The risk assessment should also validate the vendor's evidence of its controls and help your organization determine whether those controls are adequate to provide specific products or services.

Why Are Vendor Risk Assessments Important?

For many industries, a vendor risk assessment is a regulatory requirement. There are, however, many other excellent reasons for making vendor risk assessments a standard practice for your organization. By performing a vendor risk assessment, your organization can evaluate risks in advance and take appropriate steps to address them before they impact your business or operations. Additionally, failing to conduct vendor risk assessments can have disastrous consequences, including legal action and reputational damages.

Understanding Vendor Risk and Criticality

Inherent Risk

The inherent risk is the risk that naturally occurs when your organization outsources a product or service to a vendor. After all, every product or service has at least some risk. Essentially, inherent risk refers to the raw or untreated risk associated with a product or service and is identified through your internal inherent risk assessment.

Here are a few examples:

- If the product or service requires access to your customer's sensitive or confidential information, there are **information security risks**.
- There are **compliance risks** if the product or service is subject to legal or regulatory requirements.
- If the vendor interacts with your customers, **reputation risks** exist.
- There are **operational risks** if the product or service is required to support your day-to-day business.

As risks are identified, the level or severity of those risks is initially considered without regard to any risk mitigation controls. An internal inherent risk assessment is necessary to help your organization assign a risk rating or level to each identified risk. Most organizations use a risk rating or level scale of low, moderate, or high.

Criticality

Identifying whether the product or service (and overall vendor relationship) is critical to your operations or customers is also important. An organization's critical vendors are those that would cause serious operational issues or negatively impact your customers if they were to fail or have a prolonged outage. To determine if a vendor is critical, you can ask the following questions:

- Would the sudden loss of this third party cause a disruption to our organization?
- Would the sudden loss of this third party negatively impact our customers?
- If it takes longer than 24 hours or one business day to restore services, would there be a negative impact on our organization?

If you answer "yes" to any of the above, you're probably dealing with a critical vendor.

When determining criticality, your organization may need to consider other factors, such as:

- Would a change of vendor or bringing the outsourced activity in-house require significant resources, finances, or time?
- Would our organization be subject to regulatory scrutiny, enforcement actions, or fines if this vendor failed to deliver its products or services?
- Could this vendor's failure damage our organization's brand or reputation?

Knowing your vendor's risk level and criticality is important, as these two factors inform your organization how the vendor relationship must be treated and managed. Everything is determined by the vendor's risk level and criticality, from the scope and depth of due diligence to the frequency of risk re-evaluation and contract structure. Critical and high-risk vendors require the most robust due diligence, risk re-assessment, and management. Auditors and regulatory examiners often focus on critical and high-risk vendor relationships.

Common Types of Vendor Risk

So, what are the specific vendor risks your organization must identify and manage? There are many risks to consider, but here are examples of the most common vendor risk types:

Strategic risk occurs when a third party's actions don't support your organization's goals and objectives, can't be tracked effectively, or provide a positive ROI.

Reputation risk occurs when the third party interacts directly with your customers or if the third party's actions can impact how your customers perceive your organization.

There is operational risk if a product or service is essential for your organization to perform normal operations. Some organizations regard operational risk as an overarching risk category that covers information security, business continuity, and disaster recovery risks.

Cyber/information security risks are present whenever vendors access, transmit, process, or store your organization's (or your customer's) sensitive data. Additionally, vendors may pose physical information security risks if they access your data centers, offices, or other facilities.

Your third party poses **financial risk** to your organization when they suffer from poor financial health. Declining financial stability may impact the vendor's ability to provide your products and services per acceptable and contractual requirements.

Regulatory/compliance risk occurs whenever laws or regulatory requirements govern your industry or the product/service the vendor provides. Remember that your organization can be held liable for your third party's legal or compliance violations.

Additional risks emerge as the vendor risk landscape continues to evolve, so it's important to consider whether your risk assessments need updating. Organizations are considering newer risk categories such as ESG (environmental, social, and governance), geopolitical, and concentration risks, to name a few.

The Vendor Risk Assessment Process

A vendor risk assessment begins when specific types and amounts of risk associated with a product or service have been identified through your internal inherent risk assessment. Your vendor risk assessment is meant to verify that your vendor has appropriate risk management practices and controls to mitigate those inherent risks effectively. The vendor risk assessment also helps your organization verify that the vendor is a legitimate business entity with a solid reputation. Let's look at the tools and resources necessary for a vendor risk assessment and the steps in the process.

Vendor Risk Assessments: A Snapshot of the Process, Tools, and Resources

- Third-party engagement risk rating and criticality
- Basic vendor information (name, address, website, location, business license, etc.)
- Completed vendor risk questionnaire
- Vendor due diligence documentation (to evidence risk management practices and controls)
- Subject matter experts (SMEs to perform the assessment)
- Issue remediation process

8 Steps in the Vendor Risk Assessment Process

Complete the inherent risk assessment and assign risk rating: The inherent risk assessment is completed to identify the types and amounts of risks associated with the product or service. Your organization must have a methodology to calculate the risks and assign a risk rating.

Determine criticality: Your organization determines if the product or service will be critical or non-critical to your operations.

Verify the vendor's business standing and reputation: As part of the vendor risk assessment process, you must validate that they're a legitimate business. In addition, understand the vendor's ownership structure (parent, affiliate, subsidiary) and if they were previously doing business under another name. You'll need to identify and confirm the locations of their corporate headquarters and all facilities used to provide your organization's products and services. The company's principles must be identified to ensure they (or the company) aren't on any sanctions lists. Finally, you'll need to investigate your vendor's reputation through internet news searches, review websites, and the Better Business Bureau.

Scope due diligence: Once you know the vendor's risk rating and criticality, you can scope the due diligence requirements. The higher the risk, the more intensive your due diligence process must be. Critical and high-risk vendors must undergo the most rigorous due diligence.

Have the vendor complete the risk questionnaire: A vendor risk questionnaire is provided for the vendor to complete. The questionnaire includes a list of comprehensive questions related to the identified risks for the vendor to answer. Those answers should provide detailed information to your organization regarding the vendor's risk management practices and controls.

Request and gather vendor documentation to evidence controls: Your vendor must provide documented evidence of their risk management practices and controls. The documents you request will vary depending on the risks identified. Commonly requested documents include policies, procedures, independent third-party audits, audited financials, business continuity, disaster recovery plans, employee training, and background checks.

Subject matter expert reviews: Once the questionnaire is completed, and the requested documents are received, subject matter experts can review the provided information. SMEs are typically certified or credentialed professionals specializing in a specific risk domain, such as compliance, information security, finance, etc. They're responsible for evaluating the sufficiency of the controls and providing a qualified opinion as to whether the organization should proceed with the vendor relationship. They also identify issues that require remediation before or after the contract is signed.

Issue remediation: Any issues discovered in due diligence must be addressed. It's important that remediated issues are reviewed and approved by the SME before they are considered closed. As a best practice, issues must be remediated before executing the contract. However, there may be issues where post-contract remediation is acceptable. In that case, the issue description, remediation plans, and timing must be included in the contract.

Vendor Risk Re-Assessment and Due Diligence

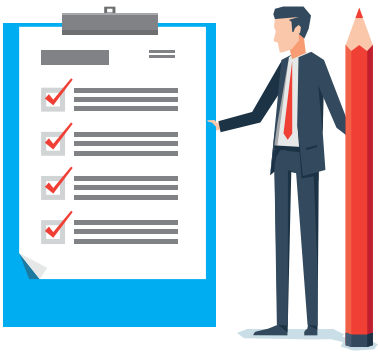
A vendor's risk profile is never static. Many circumstances can influence how risk shifts and evolves. Changing regulatory or industry standards, financial health, loss of key personnel, mergers and acquisitions, consumer preferences, and negative vendor news can all impact vendor risk. Additional factors, such as cyberattacks and data breaches, business interruptions or outages, aging technology, and declining vendor performance also determine the amount of vendor risk to be managed. For these reasons, it's essential to re-assess vendor risk periodically.

A risk re-assessment should follow the same steps as the initial risk assessment. However, in the case of re-assessment, you may consider asking your vendor to review and update their risk questionnaire and due diligence documents vs doing everything over from scratch. In any case, the information you utilize for the re-assessment must be the most recent. Suppose new or emerging risks are discovered during the process. In that case, you may need to request additional information and documentation to complete the assessment. Remember that critical and high-risk vendors require the most robust assessments. Your organization will also need to provide evidence of each assessment and the findings from the SME review.

Your organization must also establish and document the re-assessment cadence by risk rating. For critical and high-risk vendors, it's recommended to conduct annual risk re-assessments and due diligence. However, your organization shouldn't hesitate to initiate off-cadence assessments under the following conditions:

- If there are material changes to regulatory or industry requirements
- The vendor's financial health is declining
- The vendor has poor performance
- The vendor has suffered a data breach or other cyber attack
- There is substantial negative news about the vendor
- There are increasing customer complaints about the vendor
- The vendor has been part of a merger or acquisition
- There's an upcoming any contract re-negotiation or renewal

Vendor risk assessments are integral to vendor risk management. In addition to being a regulatory requirement for many industries, they're also universally recognized as a best practice. Every organization can benefit from identifying and understanding the risks associated with all products and services as well as the vendors that provide them. A standardized and repeatable vendor risk assessment process is essential to protect your organization and customers from avoidable risks.



Download samples of vendor Control Assessments

and see how Venminder can help reduce your third-party risk management workload.

Download Now

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.