Guide to the **Vendor Onboarding Process**

venminder

Guide to the Vendor Onboarding Process

The first stage in a third-party risk management (TPRM) program is onboarding a new vendor. There's often a sense of urgency to onboard the vendor quickly, but it's essential to proceed through the process with careful planning, consideration, and collaboration between both parties. This will ensure the relationship between your organization and the vendor starts off on the right path.

This guide provides an overview of the onboarding process, with best practices and considerations for each phase. The activities presented here are designed to be repeatable and scalable for organizations of all sizes, although keep in mind that this isn't an all-inclusive list. Your organization may have additional vendor onboarding needs that aren't addressed in this guide, so consider how the following activities can be integrated into your existing processes.

Phase 1
Planning & Risk Assessment

The onboarding process will be most effective when you begin by planning for the vendor engagement and assessing the vendor's inherent risk and criticality. The information gathered during these initial steps will help streamline the subsequent onboarding activities, such as the scope of due diligence required, and help you determine how to manage the vendor relationship throughout its lifetime.

5 Best Practices in Planning

1. Confirm the business need

It may seem redundant, but your organization should formally confirm the need for a new vendor. You might discover that an existing vendor in your inventory can provide the new product or service, in which case the onboarding process may be less extensive because of the information you have already collected from the vendor.

2. Identify the key players

Assigning duties and responsibilities will help avoid unnecessary confusion and delays throughout the onboarding process.

In general, the onboarding process will require the following roles:

- **Process owners** – These are the individuals that drive and manage the onboarding process to ensure the activities are completed correctly and on time. Process owners will typically be a combination of vendor or product owners and the dedicated vendor risk management team.
- **Reviewers** – Many onboarding activities will need to be reviewed for accuracy and compliance, which generally falls to various subject matter experts (SMEs) across different departments. Information security, project management, procurement, legal, and compliance are just some of the teams that may be responsible for reviewing the onboarding tasks and deliverables.
- **Approvers** – Consider the different levels of approval needed for each onboarding activity. TPRM regulations state that senior management and the board should be involved in critical and high-risk vendor activities, but your organization should determine the specifics of what this entails.

venminder

3. Establish a vendor selection process

Consider how your organization will facilitate the vendor selection process. These are just some of the details you may want to consider and document during the planning phase:

- Will you begin by comparing two or more requests for proposals (RFPs)?
- How will you make the final decision between two vendors that are equally desirable?
- If there's a need for an alternate vendor, will you keep one or more choices as backups?
- Who makes the final decision or approval?

4. Choose an exit strategy

It's essential to consider a plan of action that your organization will take when the vendor relationship ends. An exit strategy will usually come down to the following options:

- Replacing the vendor with an alternative
- Bringing the outsourced activity in-house
- Discontinuing the outsourced activity altogether
- Combining two or more of these options

5. Set expectations about timing

Onboarding cycle times will depend on many factors, such as the vendor's responsiveness to document requests and contract negotiations. While some of these details might be out of your control, it can still be helpful to set realistic expectations or goals about timing with the vendor and internal stakeholders. These expectations can help keep both parties on track, while also identifying potential roadblocks that need to be addressed.

venminder

Vendor Risk Assessments

After the onboarding process has been planned, you can move on to the risk assessment activities. This is essentially the phase where you evaluate the potential vendor relationship by identifying the inherent risk and classifying the criticality. These activities provide the first impression of the vendor relationship and help identify any hidden risks that can negatively impact your organization or customers.

Vendor risks that are left unmanaged can lead to significant consequences for your organization, such as data breaches, reputational damage, and operational failures.

Here's a closer look at each activity:

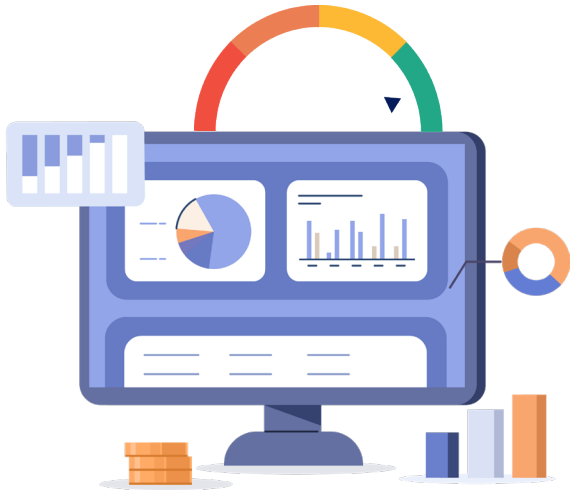
Inherent risk assessment

Inherent risk is naturally present in the vendor's product or service. Every vendor engagement will involve inherent risk, so it's essential to identify and quantify that risk through an assessment. These assessments are always done internally and are usually completed by your vendor owner.

Common risk types may include:

- **Strategic** – The vendor's actions or decisions don't align with your strategic objectives
- **Operational** – The vendor doesn't have effective internal processes, people, controls, or systems
- **Compliance** – The vendor doesn't comply with laws, regulations, or your organization's internal policies
- **Cyber and information security** – The vendor has security vulnerabilities from missing or ineffective controls
- **Financial** – The vendor's financial health is poor
- **Reputational** – The vendor's actions, lawsuits, poor service, outages, fraud, or data breaches reflect negatively on your organization

Based off the inherent risk assessment, your organization will assign a risk rating to the vendor. These risk levels are often rated on a scale of low, moderate, or high.



venminder

Criticality classification

All vendors should be classified as critical or non-critical to your operations. Criticality is not a risk rating, but rather identifies the relationships most essential to your operations and/or customers.

A critical vendor will typically fall under one or more of the following criteria:

- The sudden loss of the vendor would create a significant disruption to your organization
- The sudden loss of the vendor would disrupt your customers
- If the vendor's operations were down for more than 24 hours, this would create a material negative impact on your organization

3 Best Practices in Vendor Risk Assessments

1. Keep a detailed inventory

Vendor risk assessments include a lot of information and documentation from both the SME and the vendor. The information and provided documentation should be kept in an organized inventory.

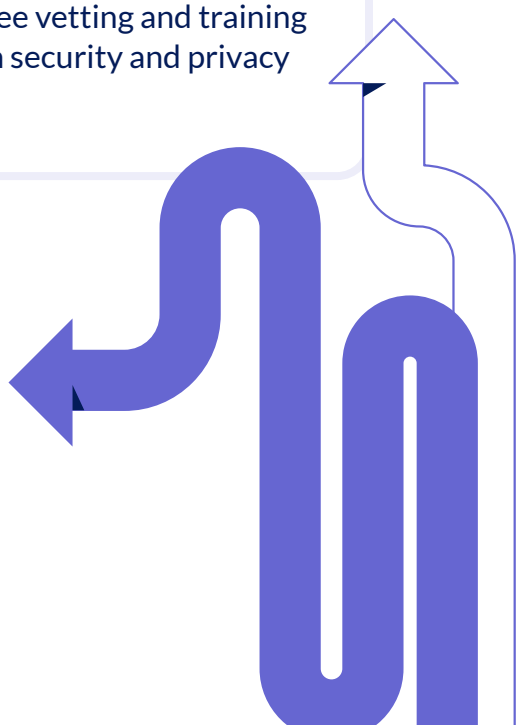
2. Verify the vendor's business standing and reputation

It's important to validate that the vendor is a legitimate business. You should understand the vendor's ownership structure, check if they've previously done business under a different name and confirm the vendor's location. You should also check the vendor's reputation through news searches, reviews, and the Better Business Bureau.

3. Ask the right questions

Ultimately, the vendor risks uncovered in the vendor risk assessment will guide the due diligence process. It's important to determine the right questions to ask the vendor to better understand the vendor's risk and how to mitigate it.

EXAMPLE:
If your inherent risk assessment uncovers cybersecurity risk because the vendor's product would be integrated with your network, you should ask the vendor questions about their human resources, employee vetting and training practices, and information security and privacy policies and practices.



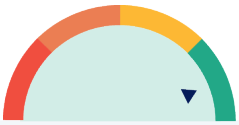
venminder

Phase 2
Due Diligence

The vendor's inherent risk and criticality classification will drive your due diligence efforts, meaning that critical and high-risk vendors should undergo the highest scrutiny. Due diligence reviews involve collecting and validating various types of information from the vendor, such as the tax ID, credit report, financial statements, cybersecurity plans, SOC reports, insurance certificates, and more.

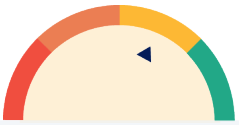
venminder

Here are some examples of what to consider collecting for each risk type:



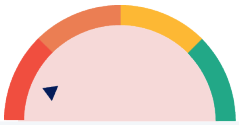
Low-risk vendors

Collect baseline documents, like business license, tax ID, credit report, Dun & Bradstreet report, OFAC checks, and negative news search findings.



Moderate-risk vendors

Collect all baseline documents, plus additional information such as SOC reports, information security policies, insurance certificates, and three years of audited financial statements.



High-risk vendors

In addition to all the items you'd collect for low and moderate-risk vendors, you should also review documents like policies and procedures, business continuity and disaster recovery plans, and penetration and vulnerability testing results.

Pre-contract due diligence is one of the most important onboarding activities, as it gives better insight into the vendor's controls and risk management processes. Due diligence is also performed periodically throughout the relationship, but this first occurrence allows you to address any concerns before signing the vendor contract.

**This is not an exhaustive due diligence list*

4 Best Practices in Due Diligence

1. Standardize your document requests

Low, moderate, and high-risk vendors should have their own due diligence requirements, which will ensure your organization isn't spending additional time on requesting non-relevant documents. Another way to create more efficiency is to establish a list of standardized documents for each risk domain and product or service type. Taking a standardized approach to document requests will help identify exactly which documents the vendor will need to provide based on the inherent risks of the vendor's product or service.

2. Consider acceptable alternative documents

In some cases, vendors may be unwilling or unable to provide certain due diligence documents. Maybe a private vendor won't disclose its financials, or another vendor hasn't yet completed a SOC report. One of the easiest ways to save time and effort is to provide the vendor with a list of alternative documents they can submit.

PRO TIP:
You can also suggest an alternative method of reviewing the documents, such as hosting a virtual session, so they don't need to submit a physical file.

3. Use SMEs to review documentation

Once due diligence documents are gathered, it's important to provide them to qualified SMEs who can accurately assess and interpret the data. SMEs are often licensed or certified in their specific risk areas.

EXAMPLE:
A certified public accountant (CPA) would be qualified to review a vendor's financial statements. They should provide a written report that details the scope of the review, the documents and information considered, and any identified gaps, material weaknesses, or other issues.

4. Create a remediation strategy

If the SME discovers any inadequacies or issues during the due diligence review, it's important to develop and document a remediation strategy.

EXAMPLE:
A critical vendor's untested business continuity plan would be an issue that needs to be addressed. Your organization should determine whether the issue must be remediated before the contract is signed. If remediation can occur after contract execution, make sure to document specific timeline requirements.

Phase 3
Contracting

Once the vendor assessment and due diligence is complete, your organization is prepared to make it official by selecting the vendor and proceeding with the contract negotiation and execution.

This phase involves two key activities:

1

Obtaining internal approvals
Refer back to your vendor selection process and solicit approval from the appropriate team or individual within your organization. The approval should be formally documented and stored according to your governance documents.

2

Negotiating and signing the contract
This can be another lengthy process, depending on the contract provisions you want to include. Some vendors will introduce standard contracts, so it's important to work closely with your legal team to ensure your vendor contract is revised as needed to include the appropriate terms and conditions that will protect your organization throughout the engagement. Critical and high-risk vendor contracts require additional scrutiny and should include some key provisions such as service level agreements (SLAs), a right to audit clause, cybersecurity protections, and more.

venminder

5 Key Provisions of Vendor Contracts:

- **Right to audit** – Throughout the vendor engagement, you'll periodically perform scheduled due diligence reviews and re-assess risks. There may also be occasions where you need to review documents outside of those periodic due diligence reviews. A right to audit clause ensures your organization will be able to collect documents from the vendor upon request.
- **Service level agreements (SLAs)** – These can vary depending on the vendor's product or service but should be clearly defined and measurable. SLAs should include details on rights and remedies if the vendor fails to meet your standards, such as termination of the contract.
- **Data breach notifications** – Regulators have set expectations for organizations to notify their customers of certain data breaches – even if the cybersecurity incident was caused by a third-party vendor. A contractual clause for data breach notifications should include details like a timeline for when the vendor should notify your organization of an incident, how the vendor will investigate the incident, and how the vendor will handle the compromised information.
- **Use of subcontractors** – Your vendors' subcontractors, or your fourth parties, should be identified in critical vendor contracts. Although your organization doesn't have a contractual relationship with these subcontractors, you can require your vendor to monitor and perform oversight on its subcontractors.
- **Business continuity and disaster recovery (BC/DR)** – Reviewing BC/DR plans should be done during due diligence, but you may want to add these details in your critical vendor contracts, too. Contractual provisions around BC/DR plans may include independent testing requirements, the frequency and availability of these test results, and your organization's right to transfer your account to another vendor without penalty in the event of business failure or interruption.

5 Best Practices for Contract Negotiation

Negotiating a vendor contract can be a challenging process, depending on what you're trying to achieve and how the vendor responds to your requests.

Keep these helpful tips in mind as you begin the process:

- **Prioritize your needs** – What are you looking to get from this vendor? What is important to you? It's important to focus first on your expectations and how the vendor will provide value to your organization.
- **Establish clear objectives** – Establish what you want to have in the contract and what you are willing to negotiate or let go of. What's a deal-breaker for you?
- **Set or know your deadline** – This will help you move the process along. Are you in a hurry and willing to concede to some of their terms? If the vendor is in a hurry to meet quota, this can give you leverage.
- **Negotiate gradually** – This will help break the process down and allow each party to not be overwhelmed with changes.
- **Move on** – Be willing to move on and walk away from the negotiations, as this may push things in your favor. Perhaps you can move to another vendor that suits your needs better. If the contract negotiation is this difficult, how will the relationship be throughout the lifecycle?

venminder

Final Administrative Tasks

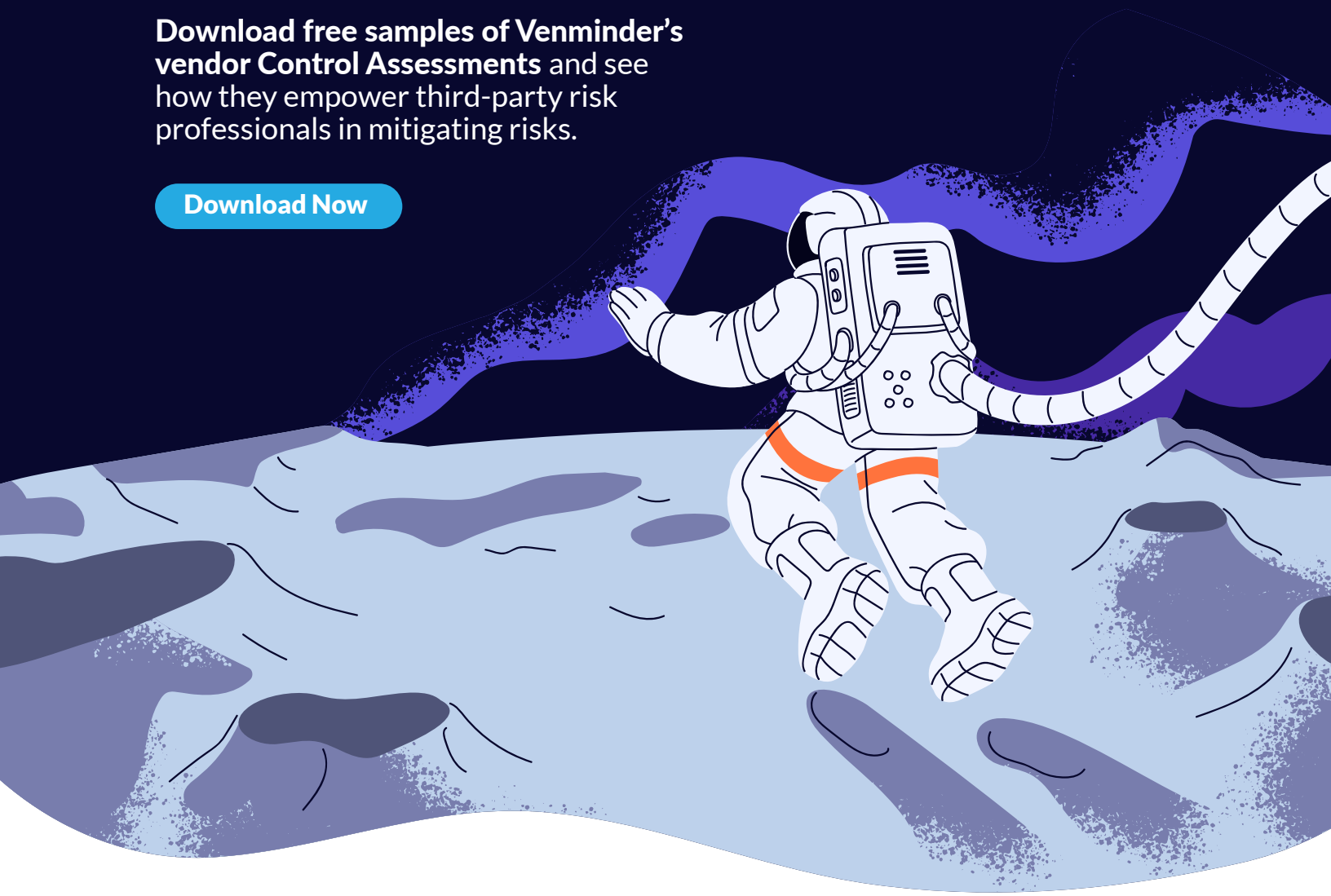
The onboarding process will generally end with any final administrative tasks that are completed internally. These will be unique to your organization, but here are a couple to consider:

- **Add vendor to internal systems** – Make sure the new vendor is properly recorded and categorized in the appropriate systems, which might include your accounts payable program, an information security system, and a TPRM platform. Also, be sure to document the official onboarding date for your records.
- **Notify the stakeholders** – The vendor onboarding process can be weeks or months long, so it's a good idea to notify your stakeholders once everything is complete. This can help avoid any unintentional delays for projects that are dependent on the new vendor.

Bringing a new vendor into your organization can present many exciting opportunities, but it's important to be thorough and deliberate throughout the onboarding process. When your vendor relationship begins on a strong foundation of planning and due diligence, your organization will be better prepared to reap the benefits of this partnership.

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

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.