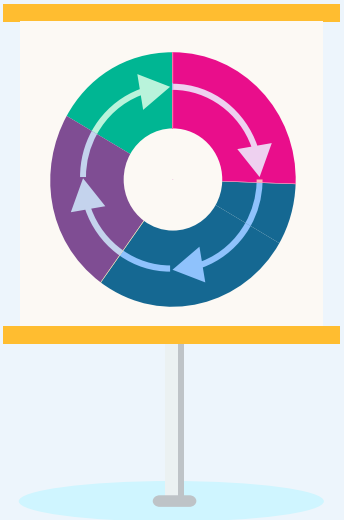
12 Ways You Can Improve Your Third-Party Risk Management Program

venminder

Expectations and requirements for third-party risk management (TPRM) are rapidly evolving. Because of this, there is always room for third-party risk management program improvement.



Here are 12 practices you can implement to improve your third-party risk management program:

01

Follow the third-party risk management lifecycle.

The third-party risk management lifecycle is a step-by-step guide for identifying, assessing, and managing third-party risks throughout the lifetime of the vendor relationship, and an excellent roadmap details necessary activities and the order in which they should occur. The three main stages of the lifecycle are:

ONBOARDING: It's essential to plan for a vendor relationship. This includes determining if the product or service is within the scope of your TPRM program, and that a designated vendor owner is assigned to the relationship. During the inherent risk assessment, a vendor's products and services are formally assessed for the types and quantities of risks and your organization will need to determine if those products or services will be critical to your operations or customers.

When the risk and criticality of the product or service have been determined, it's time to conduct vendor due diligence. The scope of due diligence is based on the risk and criticality of the engagement. The due diligence process involves gathering information from the vendor and having qualified subject matter experts (SMEs) review it. The SMEs must confirm that the vendor's risk management practices and controls are acceptable. If they are, you can officially select the vendor and negotiate, approve, and execute your contract. Once the contract is complete, you move into the ongoing stage.

ONGOING: During this stage, the vendor's risk and performance are regularly reviewed and assessed for new and emerging risks. Communication and setting expectations are key at this stage to ensure your vendor achieves the expected level of performance. Vendors and vendor owners must understand how to meet service level agreements (SLAs). Corrective actions or additional risk mitigation must occur whenever there are risk or performance issues.

OFFBOARDING: You need a formal offboarding process to avoid loose ends and gaps in your operations, no matter the reason for terminating a vendor. Exit strategies may include accounting for replacement vendors, bringing the outsourced activity in-house, or terminating the activity. During the offboarding process, data must be returned or destroyed, and vendor records must be retained. Ensure that vendor data and records are properly stored and accessible for reporting purposes and auditing.

02

Assess risk at the product/service level, not just at the vendor level.

Vendors must demonstrate that they have the right business practices and controls to manage the risk of each product and service they offer. Keep the following in mind:

- Since there are different levels of risk associated with each product or service, you can be confident examiners will focus on product/service-level assessments.
- A vendor-level assessment might miss risks that can only be detected at the product or service level. If you don't perform an assessment at the product or service level, you could be exposing your organization to unnecessary risks that could have been detected earlier.

03

Risk assess every vendor and engagement.

Risk ratings are determined by the results of your inherent risk questionnaire. Most organizations use three risk ratings: low, moderate, and high. You can use the risk rating to guide you when determining the scope of your due diligence, how often to do risk and performance reviews, and what terms to include in the contract.

A vendor's risk rating is basically the same as the engagement rating. Vendors may provide more than one product or service. If this is the case, the vendor's risk rating should default to the highest risk-rated engagement.

EXAMPLE:
A hospital contracts with a third-party vendor, KleenerMachines, to rent dialysis machines. KleenerMachines also offers a daily machine cleaning and maintenance service for an additional charge. One risk assessment should be performed on KleenerMachines to rent dialysis machines. A second risk assessment should be performed on KleenerMachines for the cleaning and maintenance service. Many medical devices now have direct access to personal health information and are connected to hospital networks, which creates opportunities for hacking and other cybercrimes.

venminder

04

Identify the vendors that provide products or services critical to your operations.

Identifying your critical third parties is essential as they require the highest level of due diligence and risk and performance monitoring. They're also essential to your internal business continuity and disaster recovery planning. It's also good to remember that critical third parties are often in focus for audits and regulatory exams.

Use these questions to determine who are your critical third parties:

- Would our organization be significantly disrupted if we lost this third party suddenly?
- Will our customers be affected by the sudden loss of this third party?
- If the time to restore service exceeds 24 hours, would there be a negative impact on our organization?

If you answer "yes" to any of these questions, you're likely dealing with a critical third party.

05

Tailor your due diligence requests.

There's no one-size-fits-all approach to due diligence. Like your other third-party risk management activities, due diligence should be risk-based and consider factors like the third party's risk rating, criticality, industry, and products/services they provide. This means each third party's risk profile is different and requires different due diligence documentation. And you don't want to waste time and resources gathering unnecessary information or overlook anything that could negatively impact your organization.

EXAMPLE:

You won't need to request a food service to provide the same information as a cloud services provider. With the food service, you might ask for documents such as a health department certification and insurance certificates. In contrast, a cloud service provider must provide evidence of controls related to their information security and privacy protections, such as independent third-party audits, penetration testing results, records of outages, and data handling policies.

06

Consider fourth parties in your due diligence reviews.

Even though you don't have a contract or direct relationship with your vendor's vendors (your fourth parties), they can also pose a risk to your organization. You don't need to worry about every fourth party. However, you should certainly review the third-party risk assessments, due diligence, and monitoring of a fourth party (as performed by your direct vendor) when:

- The fourth party provides a critical service to your third-party vendor
- The fourth party has direct access to your customers or your data

07

Plan and manage your contract.

The contract is the foundation of every third-party relationship. It's unlikely that the vendor will comply with your requirements if your contract is poorly written or key requirements are omitted. Here are four recommendations for developing a robust contract management process:

DEFINE YOUR STAGES: Contract management involves several stages. It's important to identify what happens at each stage, including:

- Internal planning
- Negotiating/creating/drafting
- Approving/executing
- Storing the contract
- Managing the contract

ESTABLISH EXTENSIVE CONTRACT TRACKING: Set up automated alerts to track key contractual dates, such as auto-renewal or termination dates.

ENSURE SERVICE LEVEL AGREEMENTS (SLAS) ARE A PART OF YOUR VENDOR CONTRACTING PROCESS: Track and monitor your vendor's performance against their SLAs and other contractual terms to ensure they're meeting expectations.

CREATE A CENTRAL AND SEARCHABLE REPOSITORY: Ensure it has comprehensive reporting for all contracts.

To assist with contract management, many organizations find third-party risk management software solutions particularly useful.

venminder

08

Review and update your third-party risk management governance documents (usually a policy, program, and procedures) at least once a year.

In addition to annually, make sure your documents are updated right away if the following occur:

- A material change is made to your organization's governance or third-party risk management program structure
- New laws, regulations, or industry best practices affecting your business take effect

09

Set the tone-from-the-top.

The organization's leaders must communicate the importance of third-party risk management and make it a priority. Organization leaders should view third-party risk management as part of their overall business strategy.

Engage senior management and the board in the following third-party risk management activities:

- Reviewing the third-party risk management policy
- Assessing the third-party risk management program's progress and effectiveness
- Addressing concerns and reviewing matters related to critical and high-risk activities or vendors
- Regularly reviewing third-party risk management team's reporting and updates on significant third-party changes, new third-party concerns, etc.

10

Leverage your lines of business and subject matter experts (SMEs).

Vendor owners in the line of business should be in regular communication with your third parties. As such, they'll likely be the first to know if there are any issues or if the third parties aren't meeting expectations. Maintain regular communication with the business units regarding third-party risk expectations and ask questions as necessary. In many cases, they have valuable insights to share.

SMEs possess a wealth of knowledge and industry expertise, so they should be the ones to evaluate vendor risk controls as part of vendor due diligence reviews. Seek their advice on any complex matters that may arise.

EXAMPLE: Certified Public Accountants (CPAs) might be better at spotting potential risks in third-party financial statements than people without accounting experience. Ask your SMEs to prepare an analysis with their findings to assist with risk assessments and other examinations.

11

Maximize your resources.

Third-party risk management is becoming more challenging as the risk landscape changes, so you must ensure your team can keep up. By replacing inefficient manual processes with outsourcing or third-party risk management software, your organization can:

- Create a single document repository for easier tracking and access
- Standardize your risk assessments and vendor selection process
- Manage your contracts, set reminders for key contract dates, and automatically track and report issues as they arise
- Invite SMEs to collaborate on risk assessments
- Enhance your bandwidth by automating time-consuming activities such as document collection and by reducing the number of errors and rework inherent in manual processing

12

Communicate and collaborate with your stakeholders.

Effective third-party risk management depends on communication. Be prepared to explain the role third-party risk management plays in your organization and how it reduces risks to your operations and your customers. Represent third-party risk management as a defender and strategic partner for your organization.

If your stakeholders understand the value of third-party risk management, confirm that they know "how" to perform key processes and activities. Be open to feedback and stay agile in your thinking. When collaboration is a regular part of your third-party risk management process, you can expect better outcomes for the organization.

Third-party risk management can be complex, and building an effective program may feel overwhelming at times. However, as the old saying goes, "the best place to start is where you are." These tips will help you implement effective third-party risk management programs or enhance those already in place.

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.