Framework for a Successful

Third-Party Risk Management Program

© 2023 Venminder, Inc.

venminder

Table of Contents

Framework for a Successful

Third-Party Risk Management Program

Many organizations need a formalized process for third-party risk management (TPRM), also known as vendor risk management. Sometimes, that need arises because of a client's request or an auditor's advice. In more serious situations, the need comes from a regulatory exam that resulted in an enforcement action. Despite these expectations from clients or auditors, it's not always clear what the TPRM process should include or how it should be executed.

It's even more complicated when this responsibility is left to an employee or a small team with some connection to a vendor, but with no experience in TPRM. An organization's sourcing analysts, information security managers, COO, or administrative assistant may be given this significant responsibility. Maybe you've been given this responsibility.

If you're unsure of where to get started with TPRM, this eBook is here to help.

You'll learn the foundational components of a TPRM framework, which will help in developing your own program. This eBook contains a high-level overview of the various elements, activities, roles, and responsibilities that are essential for a successful TPRM program. You'll also learn about the TPRM lifecycle and other helpful tips that can get you organized and prepared to implement your framework.

1 Background of Third-Party Risk Management

Nearly every organization will rely on third parties at some point. Third parties are often used when an organization needs external assistance to supplement its capabilities, access specific expertise, augment its staff, or deliver additional products and services to its customers. A third party might also be referred to as a third-party vendor, supplier, or provider. Simply put, a third party is a person or legal entity outside your business that provides its products or services to your organization, employees, or customers.

Examples are software-as-a service (SaaS) platforms, commercial printing companies, or a customer service call center. Nearly every industry uses these third-party relationships, but they're inherently risky.

It's important to understand the risks that third-party vendors pose to your organization, especially since they're often used to support critical processes. Your organization is responsible for the risks associated with your products and services, even if you outsource the production to a third party.

In many industries, government agencies regulate how outsourced relationships and processes should be managed. Several laws are also in place to protect consumers, which can impact many different organizations regardless of size or industry.

> **The laws and regulations are clear; while you can outsource the activity, your organization cannot outsource the risk.**

Some of these regulators include the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (the FDIC), and the Federal Reserve Board. These regulators for the financial services industry have even joined forces to create interagency guidance on third-party risk management (TPRM). However, other industries like healthcare and higher education also have regulations through agencies like the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC). TPRM regulations have continued to evolve with the business-risk landscape. For example, cyber risk has become a significant consideration for most organizations.

2 Identify Your **Regulators**

The first step in building your third-party risk management (TPRM) framework is to determine whether you're regulated by a government entity.

It's essential to understand the regulatory requirements and expectations for your TPRM framework, since these will provide a minimum standard of what your program should include. Do an online search for more information about regulators, existing guidance, and associated requirements. Reading and understanding these guidelines will help you plan out your framework.

Let's say you're in a regulated space but you don't follow the guidance. What happens then?

Be aware that the consequences can be severe if regulators find fault with your TPRM framework and program. The penalties can vary depending on the issue and the severity of the problem.

In milder cases, you may only receive an official notice that requires you to correct the issue within a certain amount of time. This may not seem like such a serious consequence but be warned that the subsequent penalties can be much harsher if the problem isn't corrected.

Depending on the issue, regulators can issue hefty fines or even put a stop to your business activities altogether until you correct the problem. When a regulator identifies a severe issue that requires correction, your organization will receive a public enforcement action. This can negatively affect your organization's reputation, consumer confidence, and credit rating.

What if you’re not in a regulated space?

Suppose you’re in a non-regulated industry, and your program isn’t subject to the oversight of a specific government entity. You then might question what guidelines and requirements should be established for your TPRM framework. In that case, you should follow established best practices, which mirror the stringent regulatory guidelines used for the financial services industry. It’s easy to be curious why those requirements are generally accepted as best practices.

Those very structured regulatory requirements were explicitly designed and established to systematically identify, assess, and manage risk at every stage of the TPRM lifecycle. They’re constantly updated to consider emerging risks and are considered the gold standard. If you follow these time-tested methods, you won’t need to constantly re-invent a new structure to run a successful TPRM program. Your organization can be confident that you’re running a TPRM program that functions at the highest possible standard.

3 Third-Party Risk **Management Terminology**

Beginning with regulatory guidance is a solid foundation. However, you still must have a basic understanding of a few core concepts to organize your plans and prepare to build your framework.

Let's start with some fundamental definitions. If you're already familiar with these basics, feel free to skip to the next section.

? What is a third party?

A third party can go by several names. It's sometimes referred to as a vendor, service provider, supplier, or third-party vendor. These terms refer to any person or legal entity external to your organization. Some examples of third parties include service companies, independent contractors, consultants, utility companies, law firms, and even government bodies like regulators.

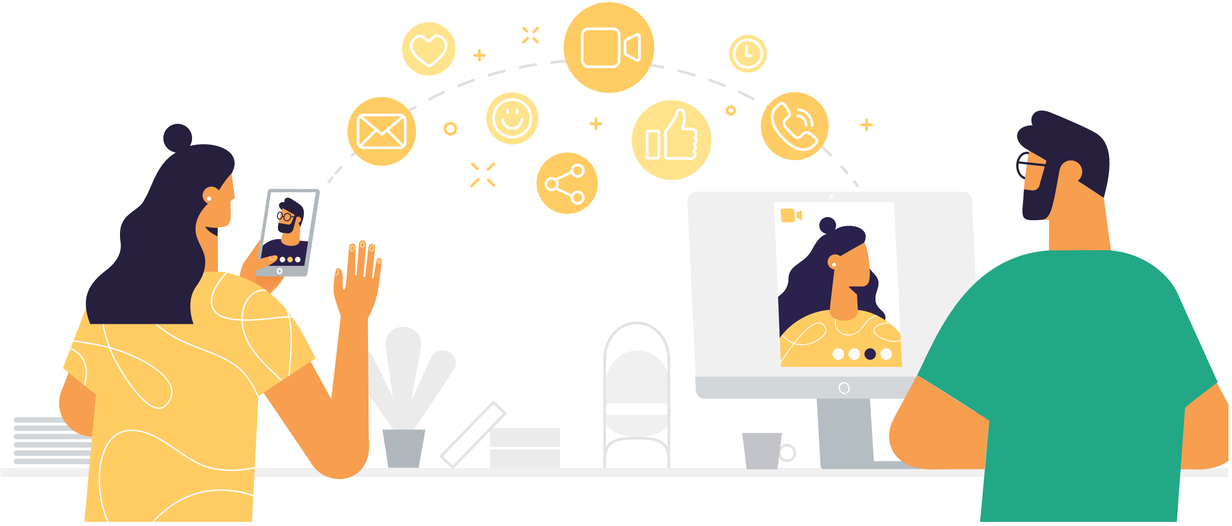
Note: *Throughout this document, we'll mostly use the term third-party risk management (TPRM), but it can be referred to as vendor risk management (VRM) or vendor management (VM) as well. Don't worry; they're essentially the same. There's no defined best practice on what to call vendor risk management, and each organization must use what makes sense to them.*

What is a third-party relationship?
This refers to a formal or informal agreement between your organization and the third party to exchange services or goods for compensation. It's important to realize that this doesn't simply mean exchanging money for a product. The services or goods can include advice, marketing, consulting, or data. The compensation can refer to monetary payment, revenue share, or endorsement. The agreement is often formalized through a contract, statement of work, purchase order, licensing agreement, or other means.

What is an activity?
The activity is also referred to as the product or service. It's a broad term that includes any task, operation, job, process, function, product, or service performed or used by your organization to support its business operations. Any product (hardware, software, or other assets) your organization uses is also an activity. Joint ventures, marketing agreements, and partnerships also fall under the category of activities. To summarize, an activity is anything your organization does or uses to fix a problem, pursue an opportunity, or maintain its operations.

What is third-party risk management?
Third-party risk management is the formalized process of identifying, assessing, and mitigating risks posed to your organization, customers, investors, or employees because of third-party activities. These risks can grow out of many different areas, including poor data management or issues related to operations or finances.

Now you have some basic terminology. Let's continue to build your understanding by introducing you to your framework's core components and some questions you'll need to answer before creating your framework.



4 Define Your **Framework Model**

Let's review the different types of third-party risk management (TPRM) models.

Having a defined model will significantly reduce rework, confusion, and frustration. There are multiple ways that a TPRM program can be used by an organization. We typically see these three models:

Decentralized

Using a decentralized model generally means you don't have a formal TPRM program or team. The various tasks like due diligence, contract management, and risk assessments are divided among different people and departments who may not be involved in collaborative reporting to the board or senior management.

Decentralized Challenges

TPRM can be an overwhelming process for a single person so it's understandable to divide the duties among several people. However, the decentralized model is still the least standardized, organized, and effective method.

There's likely no single authority to oversee the required duties, and there will always be varying degrees of consistency which can cause issues down the road for not only protecting your organization from risks, but also in dealing with auditors and regulators.

Centralized

A single team, person, or unit manages third-party risk in a centralized model. This provides more oversight and accountability of all the tasks required in vendor management. A centralized model also allows more streamlined communication between the risk management group and different organization departments.

This model must include experts from various areas, including cybersecurity, fraud, business continuity, disaster recovery, finance, and legal. TPRM is becoming increasingly more specialized so it's necessary to include appropriate subject matter experts who can manage these areas.

Centralized Challenges

A centralized model may improve overall communication but can also lead to misunderstandings if specific stakeholders are not included in the process. For example, business units may not fully appreciate the risk of doing business with a particular third party. Inconsistent communication can be a concern when they're primarily responsible for the daily interaction with the third party.

In other words, disconnection between TPRM requirements and the daily interactions between the relationship manager and vendor is possible. Items that are a high priority to you may get drowned out by the business needs or vice versa.

Hybrid

The hybrid model is recommended most often, especially for larger organizations. In this model, an organized TPRM team sets guidelines, delegates tasks to different areas, and monitors those tasks to completion. There's also an open line of communication between the TPRM team and the relationship managers.

The TPRM team will ideally work closely with the business units to ensure the consistency and timeliness of various practices. The hybrid model results in a lighter workload with consistency, oversight, and proper authority.

5 Define Roles and Responsibilities

There's a commonly used risk management principle called "The Three Lines of Defense." Some organizations, such as financial institutions, use this model to describe who is responsible for each risk management task. While it's unnecessary to use in your own framework, it's helpful to be familiar with the concept as it applies to third-party risk management (TPRM).

Three Lines of Defense:

First Line

The vendor risk is owned and managed by the first line. This line of business interacts with customers and vendors at the transaction level. They'll be the first to know if there are any problems like unmet service level expectations or unresponsiveness. A typical role in this line would be a vendor owner or vendor manager.

Second Line

The second line is essentially an organization's TPRM function that oversees the vendor risk. This line is responsible for ongoing and annual assessments, delegating responsibilities, and overseeing the entire program. A typical second-line role would be a third-party risk manager or vendor risk manager within the enterprise risk or compliance departments.

Third Line

The final and third line of defense will supervise lines one and two to ensure they sufficiently manage and oversee vendor risk.

This line will also perform internal assessments to ensure corporate policy and program compliance. The internal audit department will usually fall under this category and generally report to either compliance or enterprise risk.

While the three lines of defense model is a helpful high-level outline, it probably isn't detailed enough to use for your TPRM program. So, let's start exploring a more detailed view of roles and responsibilities.

Dedicated Third-Party Risk Management Team

Whether you're part of a team or you alone are responsible for building the framework and running the program, the general duties of the dedicated TPRM team are:

- Owning and maintaining the TPRM policy
- Reporting to senior management and the board of directors
- Ensuring the practical application of the framework, reporting, tools, risk assessments, monitoring, and termination of the organization's third parties as defined by the policy
- Reviewing and challenging first-line TPRM deliverables or activities
- Escalating issues as appropriate under the organization's risk guidelines
- Identifying emerging risk issues and apprising senior management
- Preparing for and responding to regulator exams or audits concerning TPRM
- Providing insight and updates regarding TPRM regulatory guidelines, laws, and best practices
- Engaging senior leadership to address staffing or other resource issues that prevent successful TPRM
- Ensuring the line of business TPRM deliverables are on time and of sufficient quality
- Coordinating with subject matter experts to conduct and submit due diligence risk reviews
- Ensuring vendor documentation is current and complete within the system of record

Subject Matter Experts

During the due diligence stage, subject matter experts (SMEs) are responsible for providing a formal opinion regarding the sufficiency of controls and the severity of any outstanding gaps or issues.

SMEs can either be internal employees, external resources, or sometimes a combination of both. These experts are certified in their field, which qualifies them to review certain documents and provide trustworthy feedback. For example, a certified public accountant (CPA) is well qualified to review a financial statement.

Subject matter experts are responsible for providing well-documented and authoritative risk reviews and assessing third-party controls in the following areas:

- Legal and compliance
- Information security
- Privacy
- Financial
- Business continuity/disaster recovery
- Reputation
- Cybersecurity

Vendor Owner or Vendor Manager

Usually seated within the business line, this individual manages the third-party vendor relationship on a daily basis. While actual responsibilities can vary depending on the organization, their duties would typically include:

- Working directly with the vendor to ask and answer questions
- Coordinating document requests
- Completing risk assessments
- Ensuring that due diligence is completed
- Collaborating with appropriate stakeholders to remediate issues
- Monitoring and reporting on vendor performance-related service level agreements and other performance metrics
- Reporting performance decline or emerging risk issues to management and TPRM team
- Staying current on industry regulations, laws, and news

The vendor owner is responsible for managing the vendor's risk and staying in compliance with the TPRM requirements.

Regulators

A regulator is a state or federal agency that is responsible for supervising a specific industry. Regulatory examiners closely inspect an organization's process to ensure that it covers every aspect of the TPRM lifecycle and meets regulatory rules and expectations.

Senior Management

Senior leaders throughout the organization should be involved in developing the process, procedures, projects, and reporting infrastructure for the organization's TPRM program. They should review the policy and assign people the appropriate responsibilities. They also monitor fluctuating risk levels and review service level agreement (SLA) reporting to make informed decisions.

Executive Leadership and/or Board of Directors

Board involvement isn't just critical; it's an absolute must. In fact, most TPRM guidance mandates their involvement. They should be involved with critical and high-risk vendor activities, approving your vendor management policies, and setting the "tone-from-the-top."

Auditors

Internal or external auditors are acceptable to use. They identify gaps or issues in your TPRM program before an examiner does. Auditors will also share best practices and give advice on areas that need to be changed.

Oversight & Accountability

Finally, the oversight and governance roles are accountable for ensuring the third-party risk framework operates as intended and follows regulatory laws and rules. A board of directors or executive leadership team generally determines oversight and accountability roles and requirements and communicates through official governing documents.

6 Define the Scope of the Program

You have identified an operating model and determined roles and responsibilities. The next step is creating the necessary documentation formalizing the "what, why, who, how, and when" of your framework. Before you jump in, let's take a moment to consider the scope of your framework and program. You'll need to define your scope before you write your governance documentation.

Your third-party risk management (TPRM) resources are likely limited, so having a clearly defined scope is vital to maximizing your overall efforts. The scope helps determine whether a vendor must undergo extensive risk management. This involves defining what a vendor, service provider, or third party is to your organization. Customers, clients, and specific business partner types are generally excluded from this process. As a best practice, you should establish a repeatable process to help verify all the appropriate relationships to the lifecycle by reporting the new relationship to the folks who manage it.

Recommendations to Help Determine Scope

Begin with a complete list of your third parties, which can usually be obtained from your accounts payable department. Most of your known third-party vendors will automatically be in scope and meet most of the following criteria:

- The vendor provides a tangible product or service directly or indirectly to your organization.
- There is a written agreement that details the product or service, cost, responsibilities of both parties, and termination conditions.
- The relationship is or can be influenced and managed directly by your organization.
- You have documented service level agreements related to the delivery and quality of the product or service.
- Invoices are submitted, reviewed for accuracy, and approved before payment is processed. The payment can be disputed because of issues related to quality, delivery timing, accuracy, or another specific attribute.
- The inherent risks or costs are significant and should be actively monitored and managed.

You may need to evaluate other vendors using different criteria. Consider the nature of the relationship, whether the vendor will engage with your organization, or the types of products or services it will provide.

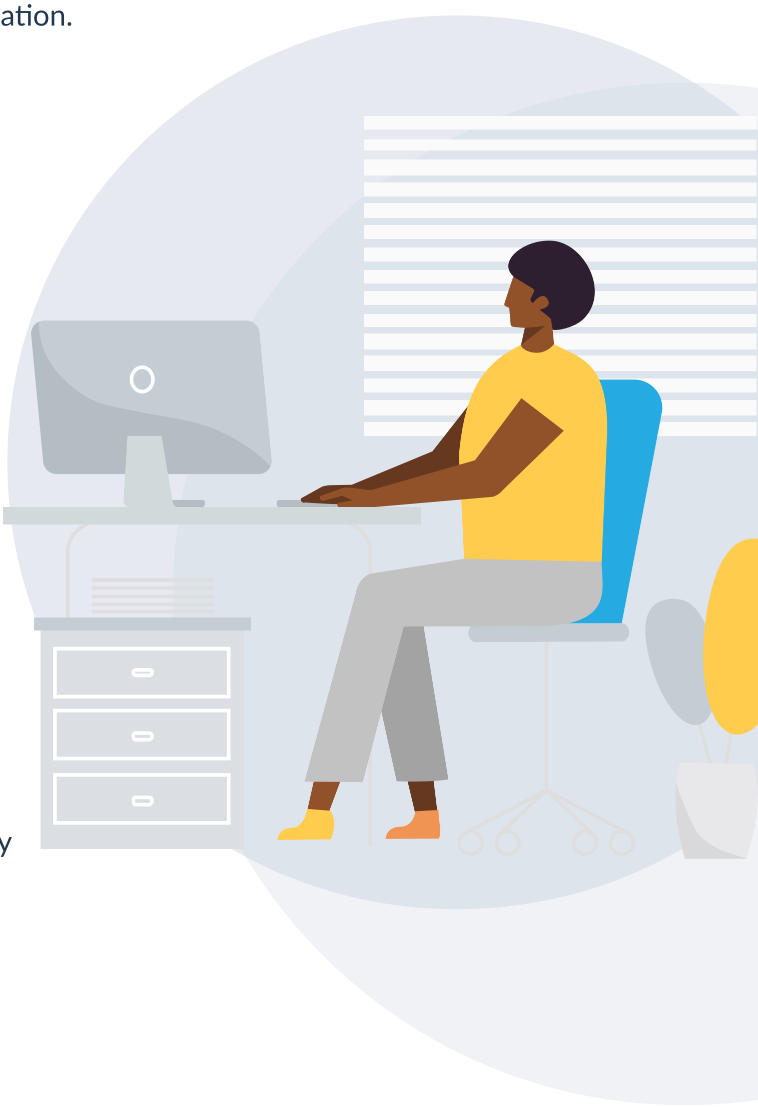
The following third-party categories and criteria are automatically out of scope:

- Government entities, including regulators, taxing and licensing authorities, and courts.
- Industry group memberships, sponsorships, donations, and events. Political donations would be managed through other internal governance.
- The vendor is limited to a single, one-time payment, known as a “payee;” litigation or payments to investors would be examples of payees.
- The vendor relationship cannot be influenced by your organization or held accountable to service level agreements. This is when you purchase a product or service “as is,” like a public utility or a lease on a property.
- Vendors that require “arms-length” methods to perform their functions appropriately, such as rating agencies or external auditors.

Other factors can determine whether a third party is in scope. The service’s scale, cost, complexity, and significance should all be evaluated. You’ll need to review the details to make an informed decision.

7 Prepare Your **Framework and Governance Documentation**

The following are standard governance documents that can be used in two ways. They can enforce the rules and communicate third-party risk management (TPRM) roles and responsibilities throughout your organization.



Policy: What must be accomplished?

A well-written policy will provide you with the foundation to build your framework. Your policy should reflect the TPRM program's minimum requirements within its current state and include details on the roles, responsibilities, oversight, and enforcement. It might be tempting to present your policy as you want to see it in the future. Still, regulators expect that you practice and enforce the program as it's currently documented. Your policy must also be reviewed and updated at least annually to reflect a maturing program.

A policy document is generally a clear description of what needs to be accomplished as an organization. Any deviations from the policy should be noted as formally approved and documented exception. A good rule of thumb would be to keep it simple, but still include regulatory responsibilities.

At a minimum, a TPRM policy would generally cover the following areas:

- Policy statement and purpose
- Scope and organization
- Roles and responsibilities
- Risk tolerance, accountability, and metrics requirements
- Risk assessment and vetting processes
- Due diligence requirements
- Contractual standards and management
- Oversight and ongoing monitoring

Program: How should the policy be implemented?

Program and procedure documents are also beneficial to your program. However, you may wait to publish them until you have a stabilized process. This will save you the time you would otherwise need to write and re-write process documents. It's inevitable that newly implemented processes will need to be changed and refined. However, it's also important to note that some organizations have very long or restrictive approval cycles for these documents. It's best to delay publishing your program until your processes and procedures are stable and tested.

A program document can supplement policy documents by further detailing how your organization should be structured to meet policy requirements. It can include the specifics of responsibilities or how different departments should work together. It also might be helpful to list the reports, deliverables, and functions needed for the process to run smoothly. This is where the metrics can be defined in more detail if they haven't been included in the policy.

Procedures: What are the steps to accomplish the program requirements?

Ideally, procedures are documents that are easy enough for anyone to understand. They should include easy-to-follow steps that produce the necessary work products and maintain operations. Think of procedures as the "how to" for day-to-day operations.

Additional Supplemental Documents:

Sometimes, additional documents are needed as they're part of the overall process and required by the governance documents. These may include:

- Information gathering questionnaires
- Risk assessment summaries
- Exception requests and reports

These document types can serve as controls and tie to audit requirements to demonstrate that the process's specific steps are fulfilled, so they're often defined as requirements in the governance documents.

PRO TIP:

Utilize Independent Reviewers

All your TPRM notes, key documents, metrics, and reports are essential to supporting and providing evidence for your independent reviews. It's one thing to have stellar governing documents in place, but they don't mean much when you can't prove that you're compliant with them. Consider outside reviewers, like independent auditors and third-party assessors, as assets that can keep you honest and help ensure your program meets regulatory guidance. They test you and your program to make sure you can prove that you're doing what you should at any given time. There's always room for improvement; sometimes, someone from the outside looking in can provide extremely valuable feedback.

8 Inventory Your **Vendors**

> **You have your work cut out for you. Still, before we move forward, there is one more task, which is perhaps the most important. You need to identify and inventory your vendors.**

As we discussed in the scope section, you must have a list of third parties in scope for your program. Suppose the details haven't already been provided. In that case, you may need to partner with your accounts payable department to gather additional information, such as a referencing contract number, the vendor relationship owner, and the product or service provided.

Now that you have a good sense of the path forward and the work that must happen along the way, it should be a relief to know that the most significant component of the framework doesn't require you to redefine or design yet another part of it. In fact, there is no reason for you to "re-invent the wheel," as they say.

There's a time-tested methodology that most third-party risk management (TPRM) programs can easily use. It's called the TPRM lifecycle and comprises three distinct stages: **onboarding, ongoing, and offboarding.**

There is much to learn about the TPRM lifecycle. For now, we'll provide a very high-level overview for you. As you build your framework and your program becomes a reality, you will undoubtedly become an expert in this process.

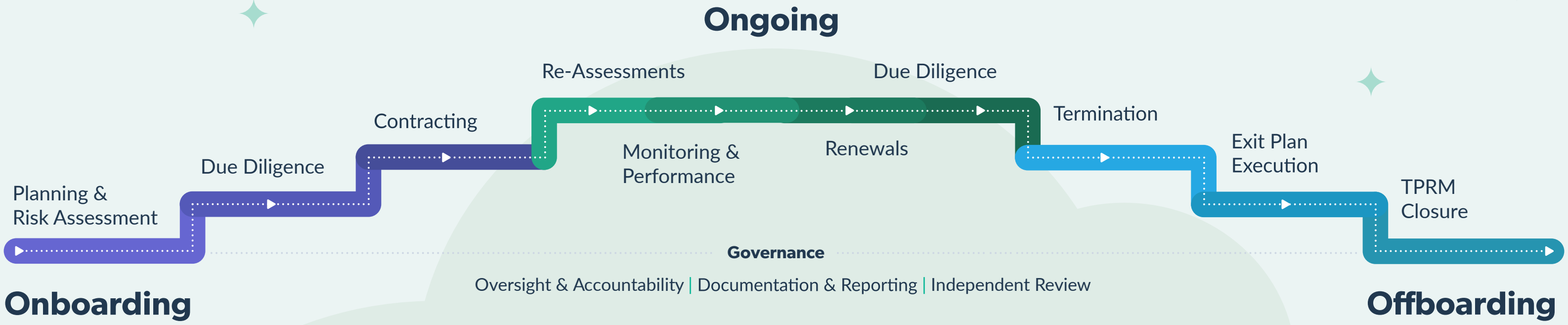
9 The Third-Party Risk Management **Lifecycle**

Before reviewing the three stages of the lifecycle, it's important to consider the foundational elements that will help guide your program. This foundation is known as governance and includes the following areas:

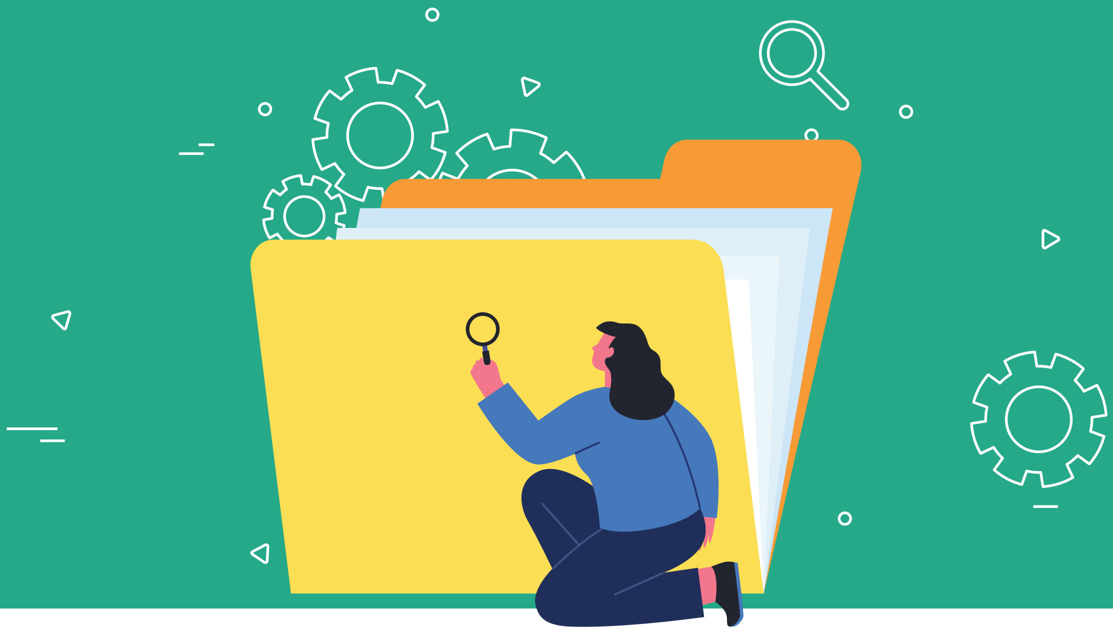
- **Oversight & Accountability** – Defines who's responsible for third-party risk management (TPRM) within your organization and how the steps and processes are managed. The board of directors or senior management typically determines these oversight and accountability roles.

- **Documentation & Reporting** – This generally includes documents such as a policy, program, and set of procedures. Good reporting is essential to any TPRM program, as it provides valuable information to the board, senior management, and other relevant stakeholders and examiners.

- **Independent Review** – Independent auditors, regulatory examiners, and third-party assessors will be helpful in reviewing your TPRM program to ensure it's compliant and effective.



venminder



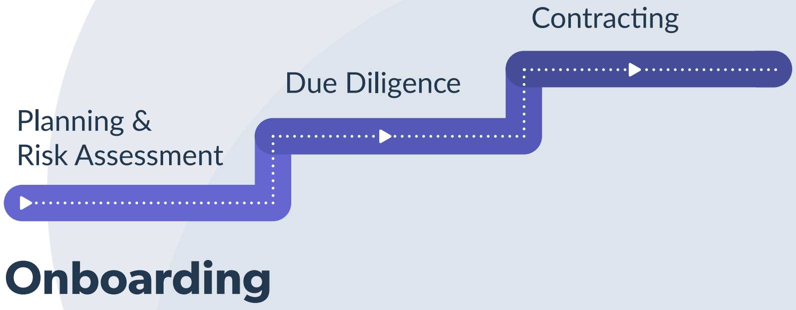
Onboarding

The first stage of the TPRM lifecycle is onboarding, which includes many critical activities that must be done prior to your official engagement with the vendor. These include:

Planning & Risk Assessment

It's important to begin with planning the relationship and understanding the highest risk the vendor could pose to your organization and whether the vendor is critical to your operations. In other words, how much would your organization or customers be impacted if this vendor performed poorly or failed altogether? Understanding those key factors is how you'll determine a vendor's inherent risk and criticality.

Not every vendor will contain the same level of risk or be critical, so each relationship needs to be evaluated and managed differently. Planning should also include the exit strategy you'll implement when the vendor relationship ends, either by terminating the contract early or simply not renewing it.



Due Diligence

Now that we understand the inherent risk and criticality of the vendor's product or service, we can determine the best way to mitigate risk appropriately and effectively. This is done by performing due diligence. This is an essential step of the process for all vendors. However, critical and high-risk vendors will generally require more extensive reviews. You should do your research and understand the vendor before entering a relationship with it.

Subject matter experts are instrumental in this process as they review vendor documentation and evaluate the controls. Your SME will assess the vendor's control environment and evaluate the supporting documentation, independent third-party audits, and other information to determine if the control environment is satisfactory and can effectively mitigate the inherent risk. These reviews are not only helpful but are required per regulatory guidance. The due diligence process will help you understand how much residual risk is present after implementing controls.

Remember that not all vendors, products, and services carry the same risk. Make sure you have appropriate and scalable due diligence requirements that are appropriate to the inherent risk and criticality.

Based on your review, you may find that all the necessary controls are in place to mitigate the risk and nothing further is needed. Conversely, you may discover that adequate standards were not met to reduce the inherent risk, so further steps will be necessary for remediation. It starts by communicating the elevated residual risk to the right people.

Next Steps When Residual Risk Requires Attention

All stakeholders, especially vendor owners, must be aware of the residual risk and open items that must be addressed and monitored. Remediation efforts and risk metrics should always be well documented. Suppose mitigation is inadequate and the vendor isn't meeting their end of the bargain. In that case, it should be escalated to senior leadership to either accept the risk or determine any further actions.

If this occurs during initial due diligence, the best and easiest solution would be to consider a different vendor, as this is done pre-contract. It's unexpected for an existing vendor's residual risk to exceed your organization's risk tolerance. Depending on the level of risk, criticality, and contract terms, these circumstances may lead to formal corrective action plans, litigation, or contract termination.

Contracting

Contracting refers to processing written agreements with third parties providing products or services to your organization. This is done after completing a risk assessment and due diligence to identify both the inherent and residual risk levels and verify that the relationship's residual risk is acceptable. For new engagements, you can safely determine which vendor is moving forward. For existing vendors, you can use the risk assessment and due diligence data to determine if any provisions should be made in the next contract review and update.

Contract management entails:

- A formal process for internal planning, negotiating, creating, drafting, approving, executing, storing, and managing contracts
- Incorporating essential controls
- Creating service level agreements (SLAs)
- Managing key contractual dates

Contract Management Importance

Properly managing your contracts will save money, time, and other resources and help you avoid unnecessary headaches like missing important contract renewal and expiration dates. Contract management also establishes expectations to ensure your organization is protected from all areas of vendor risk.

How to Handle Contract Management with New Vendors

When negotiating new contracts, you can begin with your standard template or use one provided by the vendor templates. Be sure to build upon it and change terms and provisions as needed.

Aside from your standard contract terms, here are five additional recommended terms to include in your contract:

1. **Regulatory compliance** – Vendors might not be held to the same standards and regulations as your organization, so make sure to hold them accountable to YOUR standards in the contract as much as possible.

2. **Notifications** – Ensure the vendor is required to notify you of any changes that affect your organization. For example, switching data centers that hold your data.

3. **Software service levels** – Be sure to include uptime and maximum downtime requirements for software services. You can also consider penalties if a vendor exceeds their maximum downtime, especially if the lapse in service would harm your organization (i.e., critical applications).

4. **Termination** – Having fair conditions for termination can go a long way in minimizing any future disruptions. Exit strategy provisions should be laid out in the contract and documented internally for any vendor with your data. Try to ensure the strategy covers both a gradual, intentional dissolution and a sudden loss of a vendor. Have a plan in place to replace the vendor or bring the function back in-house.

5. **Right to audit** – To the maximum extent possible, have your vendors agree in writing that they will allow you access to their policies, procedures, and facilities at least annually and as necessary if there are issues.

How to Handle Contract Management with Existing Vendors

Most regulators and auditors are looking to verify that your contract management process is well-developed, organized, and maintained continuously.

Here are four essential considerations regarding contract management:

1. **Roles and responsibilities** – These should be clearly identified.
2. **The approval process** – There should be an appropriate approval process for signing contracts, such as executive leadership-level approval for critical vendors.
3. **Pre-contract due diligence** – It's important to complete due diligence before a contract agreement.
4. **A contract repository** – Organize your contracts in a central repository so you can properly track and maintain them.

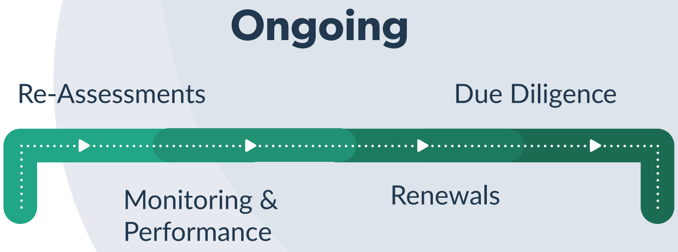
When practicing contract management, you should discuss specific details with your vendor, such as service delivery and performance, accountability of specific requirements, and any existing service level gaps.

PRO TIP:

Don't forget SLAs in contract management. Tracked and reported SLAs provide benefits to both parties by keeping them accountable.

Ongoing

Now that the vendor has been onboarded, the ongoing stage can begin. Vendor relationships can evolve with new and emerging risks, so it's critical to perform the various activities outlined in this stage:



Re-Assessments

The timing of your periodic risk re-assessments will depend on the vendor's inherent risk and criticality. Critical and high-risk vendors should be re-assessed at least annually. However, a data breach or decline in performance may warrant a more frequent schedule. Moderate vendors should be re-assessed every 18-24 months, and low-risk vendors can typically go two to three years between re-assessments or at contract renewal.

Monitoring & Performance

Ongoing monitoring of a vendor's performance and risk is often overlooked. Still, it's one of the most vital TPRM activities. This process often includes:

- Tracking and monitoring performance through service level agreements (SLAs)
- Identifying and remediating any issues or changes
- Using risk alerts and monitoring services for more targeted insight into your vendor's risk profile

You want to be prepared if things start to go astray, such as unmet SLAs, data breaches, or other incidents. You should have the necessary information and notifications set up to manage the situation promptly.

If there are changes in the vendor's internal processes or control environment for some reason, the issue needs attention quickly. It's best to closely monitor them to understand how it might affect your organization.

Six Ongoing Monitoring Best Practices

To accomplish a healthy routine of ongoing monitoring, it helps to establish these items:

1. **Regularly run reports** – Report and escalate vendor activity regularly to senior management and the board to keep them informed.

2. **Set up SLA tracking** – Track your vendor's SLAs to understand how it's performing. Set up a method to track these metrics, possibly in your TPRM platform.

3. **Use an open-source monitoring tool** – This should give notifications on significant vendors throughout the lifecycle.

4. **Base review schedules on inherent risk** – Review the vendor's highest rating and calibrate your activities accordingly. A vendor with high inherent risk but moderate residual risk should be reviewed on a high-risk frequency.

5. **Set an ongoing monitoring standard** – It should be appropriate for your organization and resources. However, a general rule of thumb would be to review critical and high-risk vendors annually, moderate risk every 18 to 24 months, and low risk every two or three years.

6. **Stick to your internal vendor management policy** – Examiners will want to see that the work product matches your policy.

PRO TIP:

Monitoring a vendor relationship is a team effort shared by business owners, third-party risk managers, or vendor owners.

Here's an overview of how roles usually contribute to ongoing management of third-party risk:

Vendor Managers or Vendor Owners – Responsible for keeping an ear to the ground, monitoring vendors for risk concerns throughout the relationship, and conducting periodic risk assessments and due diligence reviews. Their ongoing monitoring tasks include tracking SLAs and liaising with the vendor appropriately if any risk or contract issues arise.

Contract Managers – Typically maintain contracts by keeping track of key dates, such as when the contract is up for review and renewal. Suppose contract issues arise, such as not meeting contractual requirements or any concerns warranting an amendment. In that case, contract managers should be in the loop. These functions may vary or be shared somehow, depending on how the organization is structured and roles are delegated.

PRO TIP:

As long as you're leveraging a vendor for an outsourced product or service, you must maintain some level of ongoing monitoring.

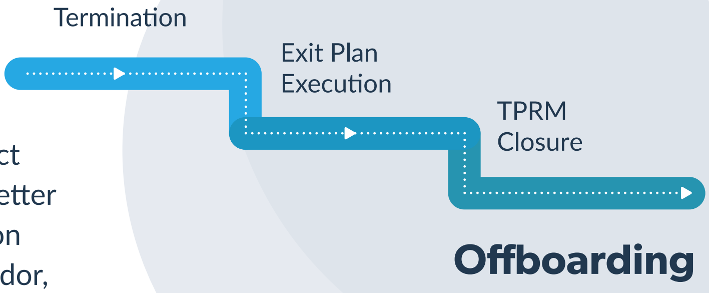
Due Diligence

Make sure that due diligence documents are continuously updated and accurate. Certain documents like insurance certificates and SOC reports have expiration dates, so it's important to periodically review your vendor's due diligence to ensure everything is current. Make sure to track any expired documentation and request new documentation at expiration. Other non-expiring documents may be collected and reviewed during the regular due diligence review. The frequency of due diligence reviews can align with the risk re-assessment schedule.

Renewals

Contracts should be reviewed mid-term to ensure you have enough time to renegotiate when necessary. You may need to consider additional provisions not included in your standard contract terms, such as breach notification requirements, regulatory compliance requirements, exit strategies for planned and unplanned terminations, and a right-to-audit clause.

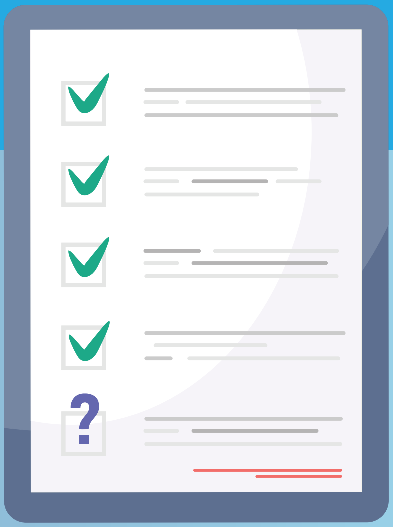
Offboarding



Finally, there often comes a time when a vendor relationship must come to an end. Maybe the contract term is expiring, or maybe you need to move on to better resources. There should always be some consideration of how the termination process may look for any vendor, especially those that are critical. The offboarding process will usually involve three activities:

- **Termination** – This involves notifying the vendor that the contract is being terminated early or won't be renewed.
- **Exit Plan Execution** – Follow your organization's pre-determined exit strategy to end the vendor relationship. This might mean that you're bringing the outsourced activity in-house, transitioning to a new vendor, or terminating the activity altogether.
- **TPRM Closure** – The tasks in this final step are primarily administrative, such as paying the final invoice and updating the vendor status in all your organization's systems. All the vendor's documents should also be appropriately organized in case you need them for a future audit or regulatory exam.

10 Moving from **Policy to Practice**



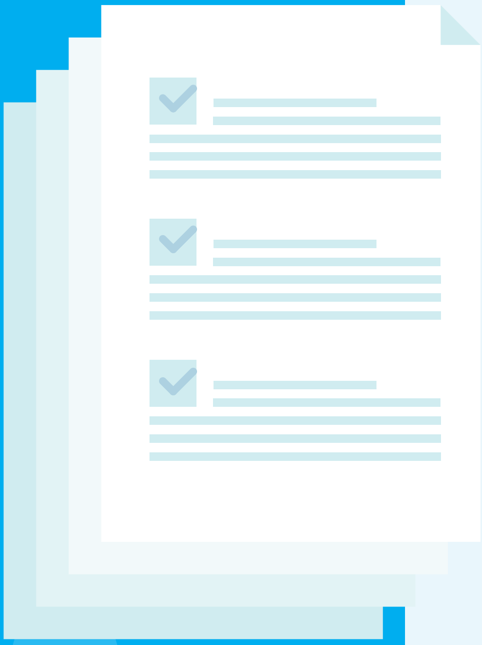
Even if you're the single individual responsible for building a third-party risk management (TPRM) framework, you'll still have to depend on many people's information and expertise throughout the process.

You'll also need the collaboration and cooperation of many different teams and functions across your organization to make the framework function correctly and as intended. Putting it all together is an enormous task, which requires additional heavy lifting to ensure all the stakeholders are on board and prepared to fulfill their everyday tasks effectively. So, how do you ensure all your hard work results in a fully functioning framework?

Here are some best practices to help you transform your framework from words in a policy to actual practice:

1. **Secure an executive sponsor.** Employ a senior leader (C-Level is best) as an official advocate for the new TPRM program. There is often less resistance to new requirements when they're promoted by senior management.

2. **Start socializing the framework early.** Let key stakeholders know that TPRM programs and frameworks are in progress. Schedule time to discuss the planned requirements and objectives and any questions or concerns your stakeholders may have. They'll provide a different viewpoint to consider when building your process, and they may have some great ideas to simplify or improve your proposed processes.



3 **Plan a phased approach.** Determine what is realistic and doable for your organization. Many of your stakeholders may be concerned with the initial workload requirements. If you break the significant work efforts down into smaller parts, your stakeholders will find it less overwhelming. However, you must hold everyone accountable and ensure deadlines are met and that the quality is sufficient.

4 **Prepare some training and education materials.** Regardless of how simple and user-friendly your new process and system may be, you must prepare to help your organization understand why TPRM is necessary and the value it brings. After those two concepts are well understood, you can begin educating the team on performing the required processes and tasks.

5 **Get feedback.** TPRM can be a challenging process for some people. If they're very vocal about their concerns and struggles, it can send the wrong message about the value of your program. Make sure you listen to feedback objectively. Let your stakeholders know if the feedback can be used for improvements.

6 **Mature your program through continuous improvement.** Building a TPRM framework is no easy task. Once it's in place, you must continually evaluate what improvements can be made. For example, you want to ensure your vendor managers can easily understand and perform their required tasks. Additional training, adjusting workflows, or re-writing procedures can help secure their understanding. Suppose your documents and records are all managed through a manual process. In that case, you may wish to investigate the benefits of a TPRM SaaS platform that will provide a single document repository and automate workflows and reporting.

There are many steps to building a solid TPRM framework.

We have only scratched the surface here. Still, after reviewing the essential information, definitions, best practices, and important considerations, you should feel more prepared and confident to start building yours.

Download free samples of vendor Controls Assessments and see how Venminder can help you 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.

© 2023 Venminder, Inc.