Creating Your Third-Party Risk Management Program:

A Step-By-Step Guide

venminder

Table of Contents

Creating Your Third-Party Risk Management Program: A Step-By-Step Guide

Have you been tasked with building a third-party risk management program from scratch? The task isn't easy, and can't be accomplished overnight. Developing and implementing a third-party risk management program requires considerable planning, coordination, and as they say, good old-fashioned hard work.

Even though it can be challenging, it's not impossible if you understand who needs to be managed, what standards must be met, and who is responsible for executing the processes. You may think, "That all sounds great, but how do I get started? What do I need to do?"

This guide is for you if you're ready to develop your third-party risk management program. You'll learn how to build a third-party risk management program that meets regulatory requirements and best practices and helps your organization manage third-party risks effectively.

If you're ready, let's begin!

Introduction to Third-Party Risk Management

Third-party risk management is the practice and process of identifying, assessing, managing, and monitoring the risks posed to your organization and its customers by your third-party relationships.

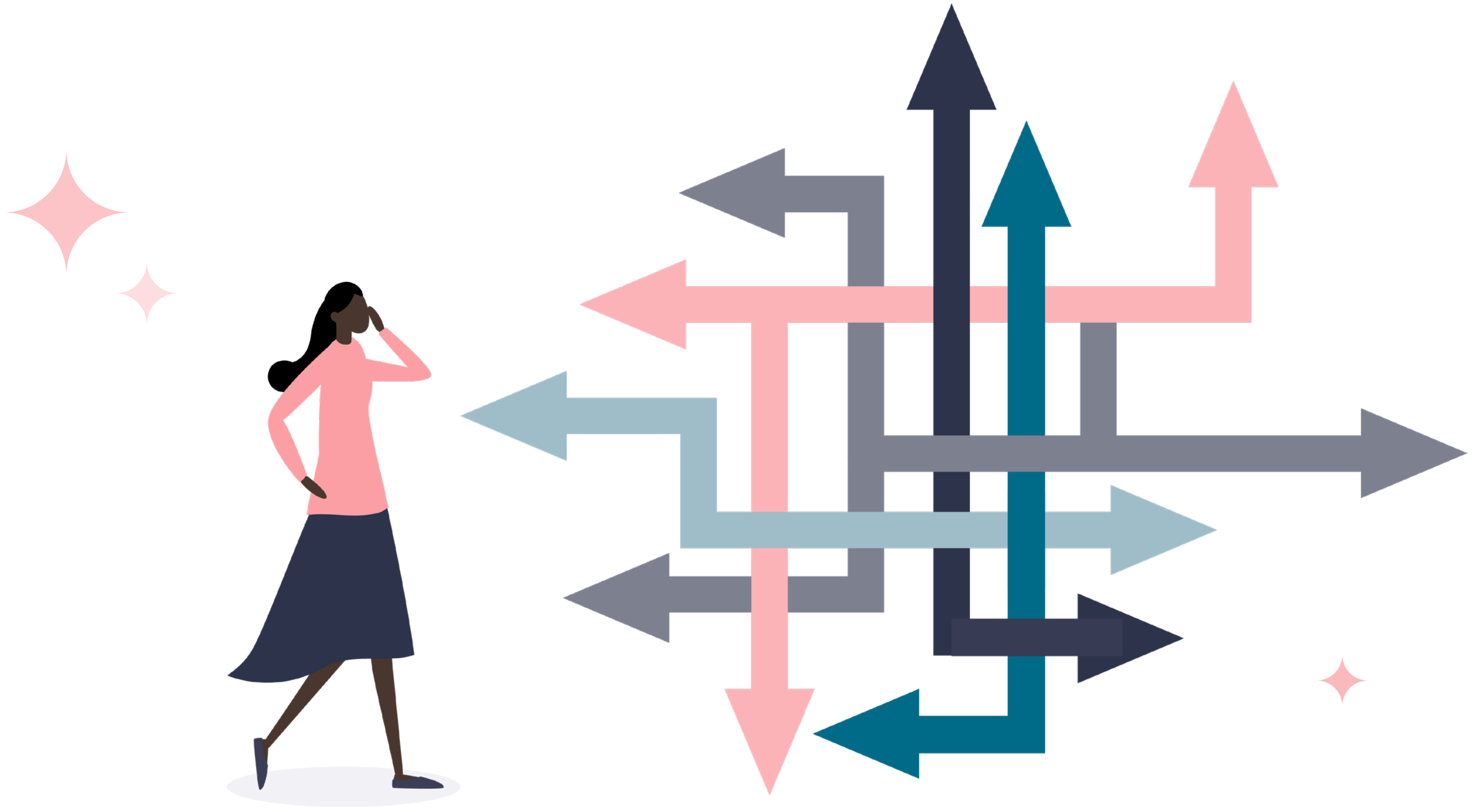
In concept, this sounds relatively straightforward. However, in execution, it requires multiple interdependent processes, the participation of various stakeholders, program documentation, oversight, and governance. Third-party risk management also requires you to know who all your third parties are and determine which ones will be in scope for your program. All of these elements come together as a third-party risk management framework.

What Is a Third Party?

Let's begin by defining the term third party. A third party is any legal entity or individual who provides products or services to your organization or customers on your behalf. Depending on your organization, you may use different names for third party (e.g., vendors, service providers, or suppliers). While some organizations may have the taxonomy to distinguish a vendor from a service provider, for example, most organizations don't make any distinction. That is why the term third party works well and can refer to any external business relationship.

How you label these relationships isn't as important as it is to identify them and integrate them into your third-party risk management practices. And speaking of those practices, you can refer to them as third-party risk management, vendor risk management, supplier management, etc. Whatever works for your organization is fine as long as you're consistent and the term is well understood across the organization.

For purposes of this guide, as we move forward we'll refer to those relationships as third parties or vendors, and we'll use the abbreviations of "TPRM" or "VRM" to refer to the program.



Getting Started Using a Stepwise Approach

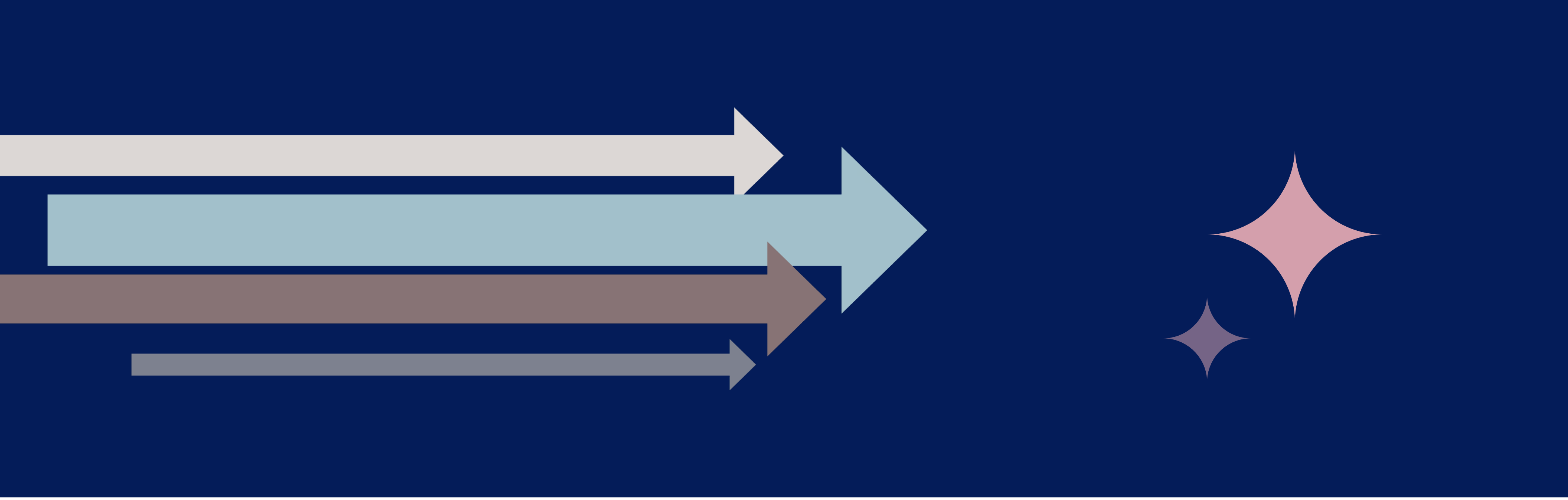
In some respects, building a TPRM program from scratch is often easier than fixing an existing one. However, it requires a thorough understanding of what the program should achieve and careful consideration and planning to ensure that processes are built and layered onto one another correctly.

To ensure success, it's best to use a stepwise approach. This means you tackle one step or process at a time and ensure it's correct before moving on to the next stage of program development. That is not to say that you can't delegate tasks or have different team members working to develop different aspects of the program simultaneously, but you must ensure that foundational elements are developed and tested before you build in more processes.

It's always important to remember that TPRM is a practice of many interrelated processes, and each process is meant to inform the activities and requirements of the next. So, suppose a process isn't built correctly or doesn't achieve its specific goal. In that case, everything following will likely be wrong as well.

Now that you're ready to build your TPRM program, let's jump in!

10 Steps to Create Your TPRM Program



1

Identify and understand the rules, regulations, and standards for TPRM

The first step is identifying the rules and requirements that will govern the program. Suppose you're in a regulated industry – good examples are financial services or healthcare. In that case, there will usually be specific regulatory guidance and requirements for how your organization should identify, assess, manage, and monitor third-party risk. You can't build an effective program without first identifying and understanding the rules. If you know who your regulators are, then a quick visit to their official website is usually the best way to find those requirements. You can also ask your internal compliance department for help or do a quick internet search. Once you have located the regulatory guidance, read it carefully. You must understand the requirements before you can meet them.

If your organization is not regulated, that doesn't necessarily mean you don't have to follow those rules. Suppose you provide products or services to clients in regulated industries. In that case, you'll be expected to adhere to your clients' TPRM standards. Even if there are no identified standards for your organization, it is wise to follow the best practices outlined in this guide.

2

Create your third-party inventory

Do you know who your third parties are? Identifying the relationships that require management and oversight should be one of your first steps. The best way to do this is to work with your Accounts Payable department. Have them provide a list of everyone that has been paid for anything in the past three years. Hopefully that list will include the product or service provided and the individual within the organization that owns that relationship. You'll need as much information as possible about those relationships to create a comprehensive third-party inventory.

When creating your third-party inventory, keep the following in mind:

- ✓ Look for third parties providing more than one product or service.
- ✓ Identify the specific product or service being provided by the third party.
- ✓ Identify who is responsible for the third-party relationship, and in cases where the third party provides more than one product or service, you may have internal owners at the engagement level vs the relationship level.
- ✓ Ensure you have the third party's contact information, including the corporate headquarters address, phone numbers, email addresses, website, etc. Double check with your Accounts Payable department that the information provided isn't just the vendor's remit to address. Suppose your AP department can't provide these details. In that case, you'll need to depend on the individual responsible for the relationship to gather that information.
- ✓ Collect contract information, purchase order numbers, or other details that help you define the third-party type and product or service.

3

Define the scope of your program

Now that you have your third-party inventory, it's time to determine which third-party types will be in scope for your TPRM program. You might think that TPRM is meant to manage all third parties regardless of type, but that isn't necessarily so. The truth is that all third-party relationships can be effectively managed in your TPRM program and, therefore, will be out of scope.

Typically, the following third-party relationships are out of scope:

- **Government Entities:** State, provincial, and similar governments can be eliminated with any organization that exercises executive, legislative, judicial, administrative, and regulatory functions. This includes any organization providing safety or emergency services, such as police and fire departments.

- **Public Utilities:** Your local power, water, garbage collection, and other public utilities are typically out of scope. Keep in mind that the key word here is public, as in it's available to everyone. Vendors providing specialized services to your organization, such as backup power generation, confidential document collection and destruction, or even the vendor servicing the water cooler, are in scope.

- **Sponsorships or Donations:** Sponsorships and donations are out of scope. Sponsoring a charity walk, assisting a non-profit, or placing an ad in the program for a high school musical aren't third-party relationships. The management of other types of donations, such as political donations, should be handled through other internal governance mechanisms.

- **Media Subscriptions:** All types of media subscriptions will be out of the scope of your TPRM program, including one-off subscriptions for magazines, books, newspapers, digital content (stock photography, music, etc.), industry news, or social media websites.

  Other subscription types should be in-scope for your program, especially if the data obtained through the service is used to make business decisions. For example, if you use subscription data from a credit rating agency to determine if a customer would qualify for a loan, then the vendor must be in scope for TPRM.

- **Payees:** Payees usually represent payments for non-product or service expenses. Examples include payments for a legal settlement or payments to board members or investors.

- **Professional Memberships and Conferences:** Annual dues for professional memberships and conferences should be excluded from your TPRM program.

Once you have determined which third-party types will be in scope for your TPRM program, you can adjust your inventory list accordingly.

4

Identify roles and responsibilities

Now that you know the rules and have established your program scope and inventory, it's time to identify and formalize the roles and responsibilities within your TPRM program. Every program is different, but there are some best practices to follow when defining who is responsible and accountable for TPRM activities and processes.

No matter what title you give to each of these roles, it's important to establish the following roles and responsibilities:

Third-Party Risk Management (Team or Individual): Responsible for the requirements, rules, tools, and processes required to effectively execute TPRM across the organization. Some of their responsibilities typically include:

- ✓ Owning the policy document and all the processes that comprise the TPRM framework
- ✓ Owning all technology platforms, templates, reports, etc., that facilitate TPRM
- ✓ Overseeing the TPRM processes to ensure they're executed properly and at the right time
- ✓ Developing TPRM program metrics and provide updates to senior management and the board
- ✓ If there is a regulatory audit or exam, they're on point for responding to documentation requests, participating in interviews, and ensuring that any findings are remediated

Third-Party or Vendor Owner: This role is typically aligned within the business line and is the individual responsible and accountable for the vendor relationship. Often, these individuals are directly responsible for the product and service provided and work with the vendor on a day-to-day basis. This role is responsible for identifying, managing, and monitoring all vendor risks throughout the relationship and they must carefully follow the rules and requirements laid out in the policy document and established by the TPRM team.

Subject Matter Experts (SMEs): These individuals can be internal or external and are responsible for reviewing and evaluating TPRM practices and controls. SMEs typically specialize in a specific risk domain, such as cybersecurity, compliance, finance, or business continuity. Not just anyone can be an SME as they should have professional credentials and certifications in their risk domain. SMEs determine whether a vendor's controls are sufficient to manage identified risks and provide a qualified opinion on whether the proposed business relationship can proceed safely. Suppose they discover issues or gaps in the controls. In that case, the SME should work with the Vendor Owner and Third-Party Risk Management to identify acceptable remediation plans.

Oversight & Governance: An organization's board and senior management will ultimately be held accountable for the effective execution of TPRM. Each of these stakeholders has a specific role to play. If your organization doesn't have a board of directors, those responsibilities default to the most senior management level. Let's discuss further:

→ **The Board of Directors:** When it comes to TPRM, one of the board's most important responsibilities is to set the right tone from the top. This means the board of directors does the following:

- ✓ Communicates TPRM as an organizational priority and incorporates it into the organization's strategy and business decisions
- ✓ Reviews and approves the TPRM policy
- ✓ Receives regular reporting and updates regarding the TPRM program
- ✓ Are kept informed of the risk and performance of vendors deemed critical to the organization's operations
- ✓ Hold senior management accountable for ensuring there are sufficient resources to manage TPRM effectively, including adequate budgets and skilled staff members
- ✓ Reviews the findings of any audit or regulatory exam and ensures senior management addresses issues effectively

→ **Senior Management:** Senior Management is responsible for communicating TPRM as an organizational priority and ensuring the program's autonomy, visibility, and support. Senior management must do the following:

- Ensure that TPRM is integrated into risk committees and that internal non-compliance is addressed
- Ensure sufficient funds are provided to obtain TPRM-specific tools, technology, services, or access expertise
- Ensure enough skilled and experienced team members to execute TPRM effectively across the organization

Independent Review: Auditors, regulatory examiners, and standard-setting bodies often perform independent reviews of the TPRM framework and its execution across the organization. If there are issues or findings, they'll be presented to senior management and the board for remediation. Or in the case of compliance violations, regulators may implement enforcement actions, including fines and other civil and criminal penalties.

5

Determine which TPRM model to use

Since every organization is different, it's crucial to determine which TPRM model will work best for yours. Defining the model will help you identify where the TPRM roles and responsibilities sit in the organization and how they work together.

There are three basic TPRM models:

Centralized
With centralized TPRM, all responsibilities are handled by a single team, such as the compliance office or the third-party risk management department. The team oversees all vendor management activities at the organization (e.g., vendor selection, contract negotiation, due diligence, performance management, and risk monitoring).

An advantage of a centralized model includes centralized responsibility and accountability, making it easier to address and remediate issues and keep everything on track. The tasks are often handled by skilled staff members, so constant training and communication outside the group isn't necessary. This can shorten cycle time and reduce errors.

However, leaving the day-to-day relationship managers out of the TPRM loop can lead to an operational silo in a fully centralized model. That can be a recipe for disaster.

A centralized approach ensures consistency, but leaving business units out can prevent them from fully understanding the risks of doing business with a third party. Additionally, those business units often have a much more nuanced understanding of the product or service and the vendor's industry, often required for the most effective risk management.

Hybrid

This model involves a well-organized and disciplined third-party risk management team setting the guidelines and checking the results of the TPRM activities, all while working very closely with the business units to ensure consistency and timeliness of practices. This approach will give you a centrally-run operation, yet a highly engaged group of business units.

The hybrid model works well, especially for very large organizations, and has several advantages. One of those advantages is more risk management involvement in the business unit.

There can be disadvantages to this model if there is not strong support from senior management. Failure to adequately fund and staff TPRM teams can mean longer cycle times for vendor onboarding and business unit dissatisfaction. These can contribute to internal non-compliance or business unit workarounds that bypass essential risk identification, assessment, management, and monitoring practices.

Decentralized

In the decentralized model, the responsibility for TPRM is spread out across multiple teams or divisions and the TPRM standards and practices may vary depending on the division. This may result in a self-customized TPRM approach for each business unit or stakeholder. While this may seem attractive, this model lacks a centralized authority for establishing the TPRM requirements and processes. It does little to ensure that regulatory or other requirements and standards are actually being met.

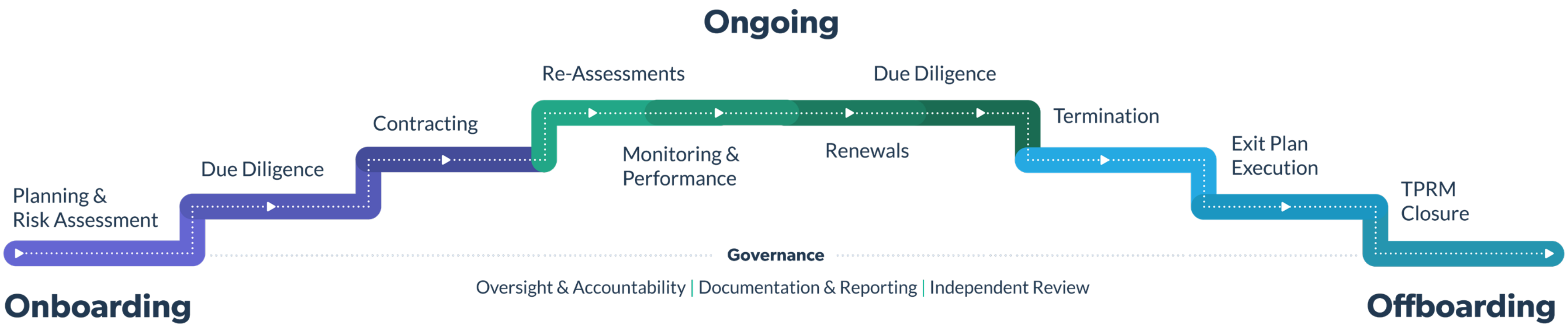
The larger the organization, the more risk there is of having radically disparate disciplines related to TPRM. It's also possible to overlook important risk identification and assessment processes when vendor selection is based on relationships, rather than cold hard facts. This can happen when a business unit is given more decision-making autonomy and there is no single source of authority over TPRM. When TPRM is decentralized in an organization, audits and regulatory exams are harder to prepare for, will take longer, and will often yield multiple findings and issues.

6

Manage risk using the TPRM lifecycle

The TPRM lifecycle helps organizations identify, assess, manage, and monitor risk throughout their vendor relationships. Originally developed by financial regulators, the third-party risk management lifecycle is now recognized as a best practice across industries.

It's the perfect roadmap for ensuring the right activities are taking place and in the prescribed sequence and is made up of three distinct life stages known as onboarding, ongoing, and offboarding. It's supported by a foundation of governance that entails oversight & accountability, documentation and reporting, and independent review.



Let's look at the foundation and the three stages of the lifecycle in more detail:

Governance is the foundation of the lifecycle and has three separate elements: Oversight & Accountability, Documentation & Reporting, and Independent Review.

Oversight & Accountability

Organizations should define who is responsible for third-party risk management, where it resides internally, and how the various steps and functions are managed. Additionally, organizational stakeholders must be educated on how the process works. Those making decisions should know how third-party risk management fits within your organization. A board of directors or senior leadership team typically determines the oversight and accountability roles outlined in the organization's official policies and procedures.

Documentation & Reporting

TPRM programs require documentation and reporting to formalize requirements, demonstrate compliance, and provide information to stakeholders. Let's look at examples of each:

Governance Documents

- ✓ **The Policy** is a high-level document that outlines the structure and concepts of the third-party risk management framework. Policies describe the program's scope, outline non-negotiable rules and minimum requirements, define stakeholder roles and responsibilities, and explain program governance. The Policy should be reviewed at least annually and approved by the board.

- ✓ **The Program** document is meant to be instructive to senior management, business lines, and other stakeholders. It should detail what is expected throughout the organization to properly manage third parties. This document will provide thorough information about the processes used to meet the policy requirements, including who is responsible and accountable for each process and any specific requirements, timing, or approvals. The program is a playbook that tells the reader who does what, when, and the tools and methods used.

- ✓ **The Procedures**, also called desktop procedures, are designed to be a step-by-step guide for executing a specific process. Procedures are generally written as a series of steps to be completed in a specific order. They should be simple so that anyone using the procedures can get the same output, regardless of prior knowledge or skillset.

Documents as evidence of compliance

Maintaining documents that evidence your compliance with your policy and processes is important. Inherent risk questionnaires, vendor due diligence questionnaires and documentation, vendor risk reviews, issue management documentation, performance management details, reports, emails, etc. should all be retained, organized, and ready for retrieval if needed, especially for audits and regulatory exams.

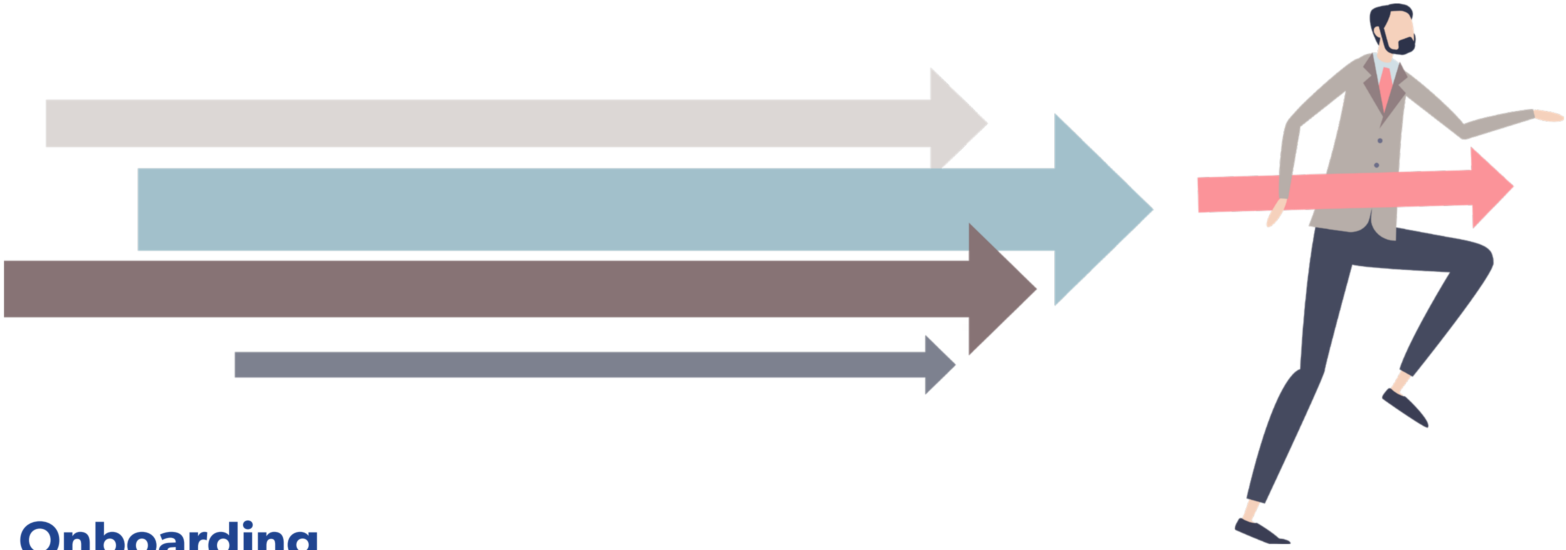
Reporting

At a minimum, TPRM reporting should be provided to the board and senior management to provide insight into the TPRM program, critical vendors, issues requiring their attention, and more. Reports can also be provided for risk committees and other stakeholders as necessary.

Independent Review

External reviewers, such as independent auditors, third-party assessors, and regulatory examiners, can keep you honest and ensure that your program complies with regulatory requirements. Outside reviewers must put your TPRM program to the test to make sure it is performing as expected. Improvements can be made anytime, and sometimes feedback from outside can be immensely helpful.

Now that we've covered the foundation of the lifecycle, let's explore its three stages:



Onboarding

The onboarding stage covers everything from the time you identify a need for a vendor, to contract execution. An important aspect of the onboarding process is identifying risks, setting expectations with the vendor, and negotiating the contract to minimize risk.

Planning: Bringing a new vendor into your organization requires careful planning and consideration from the start. You must designate an individual to serve as the vendor owner and identify what your organization will do should you need to end the vendor relationship. Would you switch to another vendor, move the product or service in-house, or discontinue it altogether?

Risk Assessment: Before selecting a vendor and signing a contract, you must understand the types and amount of risks your organization will need to manage. Best practices dictate that an inherent risk assessment is conducted before signing an agreement and determining the inherent risk and criticality is a crucial first step in any vendor engagement.

Inherent risk naturally exists as part of the product or service (and the relationship by default). This is assessed without considering any existing or future precautions or controls. Inherent risk is often rated within a tiered system of low, moderate, or high risk.

So, what are the types of inherent risks you might identify?

Strategic risk occurs when a prospective or current third-party vendor's decisions and actions are incompatible with your organization's strategic objectives.

Operational risk is broadly defined as the risk of loss resulting from a third-party vendor's ineffective or failed internal processes, people, controls, or systems.

Compliance risk occurs when a third-party vendor fails to comply with laws governing the products and services your organization provides to its customers. Compliance risk is also possible when your third-party vendor doesn't follow your internal policies, procedures, business standards, or conduct codes.

Information security risk stems from third-party vendor security vulnerabilities. Two of the most common cyber risks resulting from missing or ineffective controls are cyberattacks and data breaches.

Financial and credit risk directly relates to the third party's financial condition. Suppose the third-party vendor has insufficient investor funding, cash or credit available to meet their contractual obligations. In that case, there is a risk they won't be able to provide products and services to your organization.

Reputation risk encompasses any of the numerous ways your third-party vendor could directly or indirectly damage your reputation, brand, or company name. This harm could result from their actions, poor service, lawsuits, outages, fraud, or data breaches.

Concentration risk usually occurs when your organization has too many high-risk or critical services provided by a single vendor. This is also known as a Single Point of Failure (SPOF) risk. Another definition of concentration risk is when a significant portion of your critical vendors are located in the same geographic area. The close proximity of vendors could cause additional business continuity risk if there was a natural disaster or another external event.

Geo-Political risk occurs when your vendor is located in a country or location that is susceptible to political unrest, corruption, human rights violations, lax privacy laws, or other risks that can harm your organization or its customers.

Transaction risk exists whenever a vendor processes payments or accepts money on your behalf.

Good to know!

Inherent risks should be identified in every vendor engagement using a standardized inherent risk questionnaire. Your organization is responsible for developing its own questionnaire or adopting an existing one suitable for your organization.

Vendor criticality reflects the business impact on your organization should the vendor fail or go out of business. Products and services essential to sustain your core operations, interface with your customers, or support your organization's ability to comply with regulatory requirements are all examples of critical vendor engagements. Every vendor should be rated as either critical or non-critical.

How do you know if your vendor is truly critical vs important? Defining the specific critical vendor criteria is necessary to avoid confusion in your organization.

To begin, ask these three questions:

Would a sudden loss of this vendor cause significant disruption to our organization?

Would that disruption impact our customers?

Would the time to restore the required service exceed 24 hours, and would that cause a material negative impact on our organization?

You're likely dealing with a critical vendor if you answer "yes" to any of these three questions.

Critical should never be used as a risk rating, but rather as a way of identifying vendors whose failure would have the greatest operational impact on the organization. Make sure you define critical vendors' criteria and memorialize them in your policy, other governance documents, and training materials.

Remember, identifying both the risk and criticality are important. These two data points inform how you will treat and manage the vendor throughout its lifetime and determines how much and what types of due diligence are required, how the contract should be structured, and how often you must perform risk assessments and update due diligence documentation.

The intervals and requirements for performance management and risk monitoring are also determined by risk and criticality. In short, critical and high-risk vendors require the most robust risk identification, assessment, and re-assessment. They also require the most frequent risk monitoring and performance management.

Due Diligence: Once you know your vendor's risk level and criticality, you can scope your due diligence. The due diligence process helps your organization determine if the necessary controls are in place to effectively manage the identified risks. To put it another way, due diligence means doing your homework so that you understand the risks and have done the necessary research before formalizing a relationship between your organization and another.

The due diligence process is generally achieved by collecting and validating information from and about the vendor. Subject matter experts (SMEs) review the information and evidence of the vendor's risk management practices and controls. They also provide a documented review and their qualified opinion on whether the vendor's controls are sufficient. If issues are discovered during the review, they'll note their findings and require evidence of remediation before moving forward or recommend that the organization decline the relationship. If there are no issues, your organization can move forward with the vendor contracting process.

Good to know!

Your organization must create or adopt appropriate vendor risk questionnaires and establish standard vendor due diligence document requirements. Collaborate with your SMEs to develop comprehensive questionnaires to identify relevant information about your vendor's risk management practices and controls. Also, create a standardized list of vendor due diligence documents to be collected from your vendors.

Contracting: Contracts are one of your best third-party risk management tools, but they can only be effective when structured to protect your organization and its customers. The best way to ensure contracts are well written and can effectively mitigate risks to the organization is to create a standardized set of terms and conditions to include in every high-risk and critical contract.

These should include indemnification and insurance, a right to audit, service level agreements, regulatory compliance, handling customer and consumer complaints, cybersecurity and privacy protection, business continuity and disaster recovery planning, and more.

Once your contracts are signed, your vendor officially enters the ongoing stage of the third-party risk management lifecycle.

Good to know!

Never sign a contract before due diligence has been completed. Once you have executed the contract, you have reduced your leverage to make the vendor correct any issues. While the best vendors will show good faith efforts to work with their clients to correct issues, many vendors only abide by what is in the contract.

This means if they're not legally obliged to fix the problem, they won't. This is especially true when the issue mitigation may be costly or require additional vendor resources. Make sure due diligence is complete, and any identified issues are corrected before executing the contract.

Ongoing

After you sign the contract, ongoing monitoring of the vendor's risk and performance is extremely important. It's crucial to remain aware of and address any new or emerging risks or performance issues. The ongoing stage includes risk re-assessments and due diligence collection, monitoring risk and performance, and contract renewals.

Periodic Risk Re-Assessments: These re-assessments are necessary because vendor risk can change. This requires your vendor owner to review (and update if necessary) the inherent risk questionnaire. If there are changes, then appropriate due diligence document collection and review must follow.

The risk re-assessment process should follow a formal risk-based cadence:

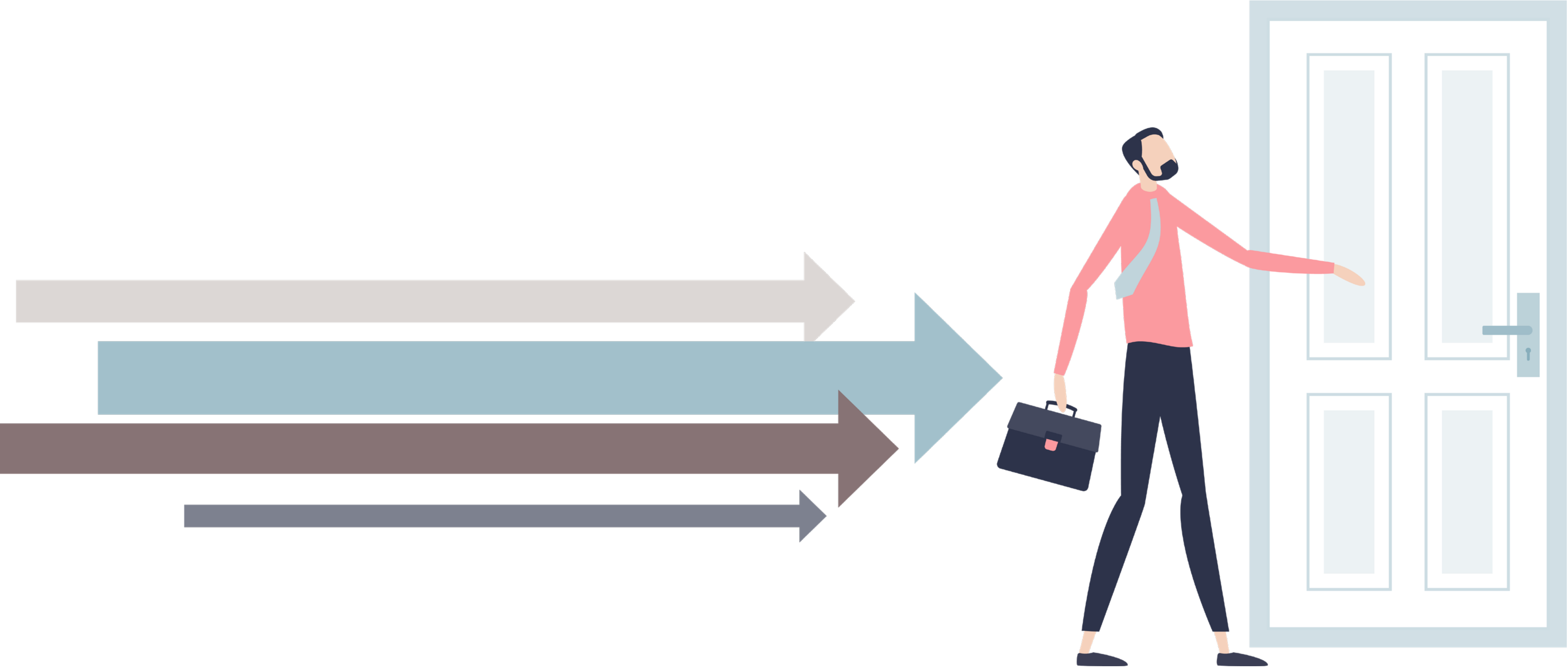
- **Critical and High Risk:** At least annually, but reviews may be more frequent if there have been issues such as declining performance or a data breach
- **Moderate:** Every 18-24 months, depending on the product or service type
- **Low:** Every three years, or at contract renewal

Due Diligence, including document collection and review: Even if there have been no changes to the inherent risk assessment, it's still important to refresh vendor due diligence documents periodically to ensure that your organization has the most current documents on file. Remember that insurance certificates and other document types, like SOC reports, do have an expiration date. For documents with specific expiration dates, it's important to track those and request new documentation as the old ones expire. Don't wait for the scheduled refresh to ensure your vendor is still insured or has tested security controls. The cadence for review should align with the periodic risk re-assessment schedule.

Risk Monitoring: Risk monitoring is necessary between formal risk re-assessments and reviews. Vendor risk can change overnight, so keeping your eyes and ears open is essential. While many organizations utilize internet search alerts to provide news on the vendor or the vendors' industry, that approach doesn't always yield the most relevant or timely information. Alternatively, your organization might consider utilizing vendor risk alert and monitoring services to provide targeted insights into your vendor's cybersecurity posture, credit rating, reputation, and more.

Performance Monitoring and Management: These are essential to ensure your organization is getting the anticipated value of the vendor relationship. Even small declines in performance can signal the presence of new and emerging vendor risk. Keeping your eye on the vendor's performance is necessary to identify and remediate small issues before they become big problems for your organization or its customers.

The activities in the ongoing stage are just that... ongoing! The activities must continue and repeat until the vendor contract expires or is terminated. If the vendor contract expires or is terminated, you move into the offboarding stage of the third-party risk management lifecycle.



Offboarding

There always comes a time when a vendor engagement must end. Maybe the engagement is ending because a vendor is bankrupt, has failed to perform, the contracted term ended, or you just need to move on to bigger and better things. You should always take into account how termination processes for any particular vendor may vary and what your organization must do to end those relationships safely and effectively.

Termination: This is the step in which you notify the vendor that the contract won't be renewed or is being prematurely terminated. Formal termination must abide by the contract terms, including notification periods for termination, who must be notified and how, and if there are fees or penalties for early termination.

Exit Plan Execution: Your organization will need to have an exit strategy identifying what it will do should there be a need to end a vendor relationship. For your high-risk and critical relationships, it's also extremely important to have a documented exit plan detailing how you will execute that strategy. An exit plan should outline the roles and responsibilities of both parties, tollgates or approvals, communication plans, and contingency plans if the vendor fails to fulfill their obligations.

Your exit plan should account for all inputs and outputs, both upstream and downstream, and ensure they're properly accounted for during the termination or transition to a new vendor.

Good to know!

The best time to build your exit plan is during onboarding. During onboarding, your organization takes the necessary steps to bring your vendor to a business-as-usual state. This is the perfect time to consider each of those steps and how you would need to reverse them when exiting the vendor.

Suppose you wait to build your exit plan during the actual offboarding process. In that case, you risk missing important steps or miscalculating the timing necessary to perform specific actions. Offboarding can be stressful, especially if it's unplanned.

TPRM closure: This is the final step in formally closing down the vendor relationship. While the tasks in TPRM closure are largely administrative, they're still essential, and might include reviewing and paying any final invoices and working with accounts payable to prevent payment of any future invoices.

The vendor status must be updated in all systems (TPRM, AP, Contract Management, Procurement, and Access Management and Provisioning systems). All vendor information and documents should be organized and archived appropriately, as you may need them in the future for an audit or regulatory exam.

7

Select the right TPRM tools and technology

As you now understand the regulatory requirements and rules, the roles and responsibilities, and the stages and required activities in the TPRM lifecycle, the biggest question is how you will effectively manage all of it? What tools or technology will you deploy to keep track of the necessary activities, manage the numerous processes, collect and store documentation, and communicate with your vendors and internal stakeholders?

Of course, there are many ways organizations manage their TPRM activities. Among them, the least desirable option is through manual processes, such as capturing and recording data using multiple spreadsheets, collecting and storing hard copies of vendor documents, and setting countless reminders on one's calendar. While it's possible to manage your TPRM processes, stakeholders, vendors, document management, and workflows this way, it's certainly not optimal.

Even though manual processes are a low-cost option for managing TPRM, they're also low-value. Manual processes are notoriously error-prone, subject to poor version control, and time-consuming. Manual processes also require more management and administrative upkeep, reducing your TPRM team's time to focus on vendor risks.

Other options include using the following:

TPRM modules that are part of an existing General Risk and Compliance (GRC) or Enterprise Risk Management (ERM) tool: While this approach is superior to manual processes, there may still be some drawbacks. GRC and ERM tools aren't all created equally, and add-on TPRM modules may not provide all the functionality required to manage the many interconnected processes of TPRM, which often means creating workarounds and off-system processes to address any gaps.

Dedicated TPRM software: This will typically provide the best solution for managing your processes and programs, as these systems are designed to specifically address the complexities and requirements of TPRM. Workflow automation, document collection, organization and storage, contact management, communication to vendors and internal stakeholders, automated reminders, and comprehensive reporting delivered through a single platform are some of TPRM software's benefits.

Whether you're building your TPRM program from the ground up or looking to make improvements, the right TPRM tool makes your life easier, boosts your risk management abilities, and enhances your program.

Good to know!

There are many TPRM software companies to choose from, so don't be shy about reviewing more than one provider. Watch a live demo of the system's capabilites, and don't forget to ask about ease of customization and how pricing is structured. Consider if the provider offers additional benefits, such as a library of risk assessment templates, user training, or live technical support.

8 Develop and implement your TPRM policy

You've done the work to identify the TPRM rules and regulations your organization must comply with, and you have created a framework and program to meet those requirements. The next step is formalizing your organizational TPRM requirements through a dedicated TPRM policy. As the foundation of your TPRM program, your policy should outline rules and requirements, roles and responsibilities, risk thresholds, issue management, and the oversight and governance necessary to ensure its success.

When writing your policy, it's always important to reflect on your current TPRM practices and processes vs aspirational ones. The policy should be reviewed and approved by your board of directors (or by senior management, if you have no board) at least once a year.

9

Monitor and manage your TPRM program

New TPRM programs often require adjustments and improvements to optimize performance and risk management outcomes. Established programs also need improvements from time to time.

Here are some recommendations for program monitoring and management:

Self-audit your program at least once a year: TPRM routines should include anticipating and preparing for audits and regulatory examinations. In addition to audits and exams, you should self-audit your program frequently.

As you audit your TPRM program, it's important to consider a few core requirements:

- ✓ Is the policy up-to-date and in compliance with all laws, rules, and regulations?
- ✓ Does your actual process align with your stated policy? (If you have a requirement in the policy that isn't being followed in practice, that should be a red flag.)
- ✓ What is the effectiveness of the processes and tools for identifying, assessing, and managing risk?
- ✓ Are processes followed consistently and are exceptions documented?

Asking these questions more can help you identify program gaps or weaknesses. Furthermore, it will allow you to improve your program before an auditor or examiner begins their assessment.

Develop and implement TPRM program metrics: TPRM metrics can help your board and management think beyond regulatory compliance, assess your TPRM program's effectiveness, and understand how risk is managed across your vendor portfolio. Data-driven metrics can also help management make decisions and drive action. The right metrics can help your management understand where there is a need for a bigger budget or additional resources or if internal compliance is a real issue.

Collaborate with and solicit feedback from your stakeholders: TPRM is a "team sport" requiring the skills and participation of different stakeholders. A more balanced and effective TPRM program is achieved by working with stakeholders, including vendor owners, subject matter experts, and other risk management teams.

10 Other considerations and best practices as you develop and finalize your TPRM program

As you finalize your TPRM program, here are some additional considerations and best practices:

Always use a risk-based approach to appropriately scope and scale your TPRM activities. Remember, the higher the risk, the more comprehensive your risk identification, assessment, management, and monitoring must be.

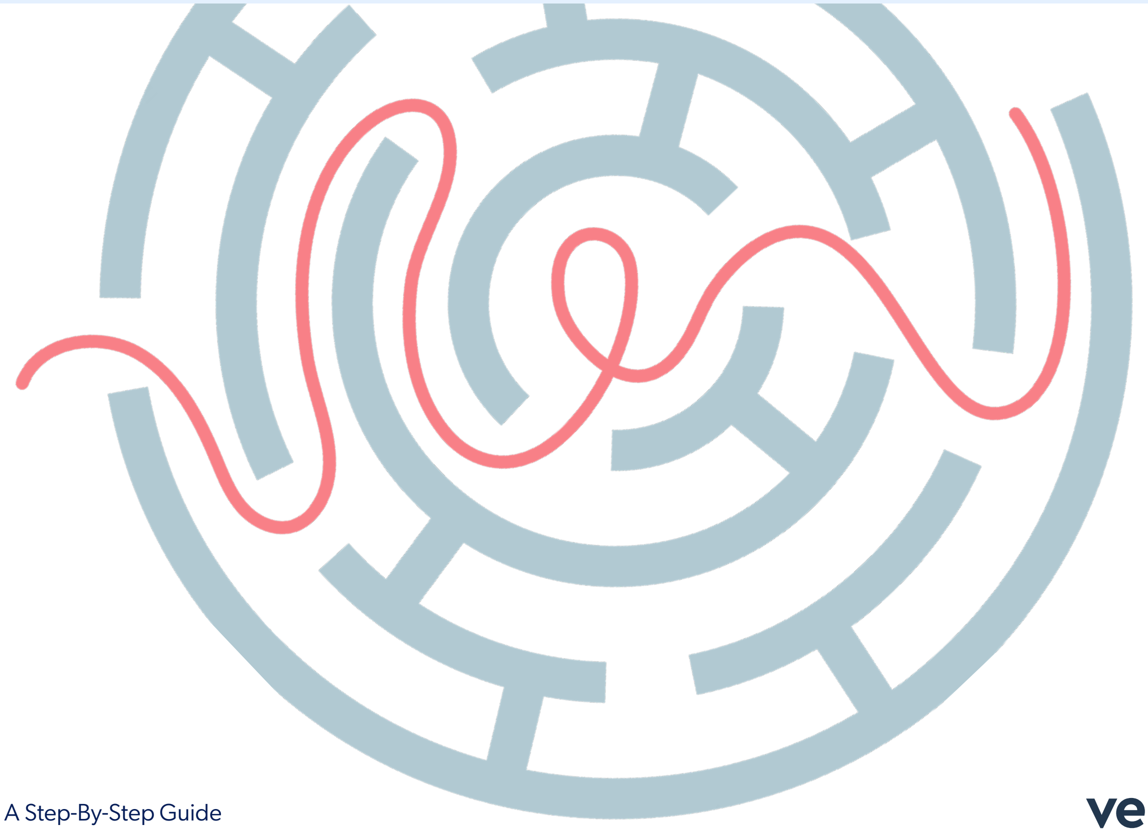
Engage the board and senior management. The success of any TPRM program largely depends on the tone from the top, meaning that the board and senior management consider TPRM a priority and integrate it into the organization's strategy and business decisions. It also means that they are regularly engaged in TPRM through reporting, updates, and approval of the TPRM policy.

Consider outsourcing to optimize existing resources. TPRM programs are notoriously lean, and it doesn't take much extra work to create a permanent backlog and create the domino effect of long wait times to get vendors up and running. Consider outsourcing to a qualified third-party risk management services provider when your TPRM team is operating at full capacity but still has too much work. You can find services ranging from due diligence document collection to contract management to supplying qualified subject matter experts to perform vendor risk assessments. Outsourcing low-value but high-effort processes, like due diligence document collection, can give your team more bandwidth to identify and manage risk.

Never stop learning. TPRM practitioners must stay current with all the new and emerging risks, including regulatory updates and changes. Invest time in learning through formal training or online webinars and workshops. Sign up for industry and regulator news alerts, research new risk topics, and talk to your TPRM peers in your industry and others.

Building a TPRM program from scratch is never an easy task.

Still, when you have the right knowledge and plan carefully, you can develop a TPRM program that not only meets regulatory requirements and best practices, but also protects your organization and its customers from unnecessary exposure to third-party risks.



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.