The Essential Third-Party Risk Management Guide

venminder

venminder

The Essential Third-Party Risk Management Guide

It can seem challenging, and even overwhelming, for organizations to manage third-party risk, but it doesn't have to be. In this guide, we'll cover the essential information you need to know about third-party risk management.

venminder

Definition of **Third-Party Risk Management (TPRM)**

Third-party risk management (also referred to as vendor risk management, vendor management, or supplier risk management) is the process and practice of identifying, assessing, and managing the risks associated with products and services provided by third parties (vendors) to your organization or your customers. This process aims to reduce risk and enhance value across third-party relationships while driving service excellence and potentially reducing costs.

venminder

Why Is Third-Party Risk Management Important?

- It's a **regulatory requirement** for many industries and will help your organization align with necessary guidelines.
- It helps your organization **mitigate risks** that could adversely affect its reputation, operations, security, and finances.
- Your organization can use it to improve **business continuity and disaster recovery** planning, negotiate and manage contracts, and reduce costs.
- In addition to helping you select the best third parties for the job, it helps you **avoid unnecessary risks** that can impact your organization and customers.

venminder

The Difference Between a **Third and Fourth Party**

Generally speaking, a third party is an individual or business entity that provides products or services directly to you or your customers on your behalf. Your third parties have a direct business agreement (contract, service agreement, purchase order, etc.) with your organization. Some examples of third parties include software-as-a-service (SaaS) providers, consultants, core processors, office supplies, and janitorial services.

HERE'S AN EXAMPLE

Imagine you have a contract with a core processor – this is your third party. However, suppose the core processor has a contract with a data storage provider where your confidential information is stored. In that case, that makes the data storage provider your fourth party.

A fourth party is an individual or business entity with a direct business relationship with your third party (your vendor's vendor). Although you don't have a direct business relationship or formal agreement with the fourth party, they may provide important services or products to your third parties that can impact your organization.

Third-Party Risk Management Lifecycle

The third-party risk management lifecycle provides an end-to-end roadmap for identifying, assessing, mitigating, and managing risk throughout the third-party relationship. Originally developed by financial regulators, the third-party risk management lifecycle is now an accepted best practice across industries.

venminder

Foundation of the Lifecycle

The third-party risk management lifecycle is supported by a foundation comprised of oversight & accountability, documentation & reporting, and independent review. Let's explore each component:

Oversight & Accountability
A key to effective oversight and accountability is clearly defined roles and responsibilities for all stakeholders. Additionally, your board of directors and senior management must establish a "tone-from-the-top," ensuring that third-party risk management is an organizational priority and holding stakeholders accountable.

Documentation & Reporting
Governance documents formally account for third-party risk management program requirements, rules, roles, and responsibilities. Your policy defines your organization's third-party risk management objectives, rules, and requirements, and it helps your stakeholders better understand their roles and responsibilities. A program document details the processes used to meet the requirements listed in the policy. Finally, your procedures provide step-by-step instructions necessary for executing your specific processes.

Reporting is also essential to any third-party risk management program as it communicates important data to stakeholders to drive action or make decisions.

Independent Review
Independent reviews help determine if your organization complies with all laws and applicable regulatory requirements. External auditors and reviewers (such as regulatory examiners) can assess your program's reports, documents, notes, and metrics to provide important feedback and areas for improvement.

venminder

Third-Party Risk Management Lifecycle Stages

Every vendor relationship has three stages: onboarding, ongoing, and offboarding. Following the third-party risk management lifecycle ensures your organization identifies, assesses, and mitigates risks throughout the vendor relationship by following the specific steps in the right sequence during each stage. Let's take a look:

Onboarding

The first stage of the lifecycle incorporates all the steps and activities you must complete from the time you identify a potential vendor up to executing the third-party contract. During this stage, you'll set the foundations for the relationship, identify the risks associated with the product or service and the third-party relationship, and assess how they may impact your organization. This includes:

Planning & Risk Assessment

Once you've determined that the third-party relationship is in scope for your third-party risk management program, it's necessary to take the following steps:

→ Assign roles and responsibilities to relevant stakeholders so that each task is given the necessary expertise, resources, and attention. Most importantly, you must identify who will be responsible for the vendor relationship.

→ Conduct an internal inherent risk assessment to identify the types and amounts of risks in the product or service and, therefore, the relationship. You must also determine if the third party will be critical or non-critical to your operations and assign a risk level or rating to the third-party engagement.

Due Diligence

Perform due diligence to verify that your potential third party is a legitimate business entity with a solid reputation and sufficient controls to manage potential risks. Due diligence is risk-based, meaning the higher the risk, the more robust due diligence should be, including:

- → Collecting and assessing basic information (e.g., tax ID, state of incorporation, credit report, OFAC check).
- → Gathering data on the third party's risk identification and management practices through a vendor risk questionnaire.
- → Collecting and assessing vendor documents that verify controls (e.g., list of their subcontractors, SOC reports, business continuity and disaster recovery plans, cybersecurity plans, financial statements).
- → Reviewing the vendor's risk management practices and controls with a qualified subject matter expert.

Contracting

Once due diligence has been completed, you can collaborate with your third party to negotiate the contract. During the contracting process, ensure you do the following:

- → Consider adding specific service level agreements (SLAs) to outline any non-negotiable standards or performance expectations.
- → Carefully consider the terms of your contract before signing, as your third party can only be held liable for terms in the contract, and your organization has little negotiating power after the fact.

Ongoing

After your contract has been signed and executed, you'll enter the ongoing stage of the lifecycle, which involves periodic re-assessments and due diligence, as well as continuous risk monitoring and performance management. Ongoing also involves the process of preparing for any contract renewals.

Due Diligence and Risk Re-Assessments

Once you've determined that the third-party relationship is in scope for your third-party risk management program, it's necessary to take the following steps:

- → Even if there hasn't been a change in the third party's inherent risk profile, all due diligence documents must be up-to-date and accurate. This includes vendor risk questionnaires, internal policies, independent third-party audit reports, financials, and business continuity and disaster recovery plans.

- → It's also essential to perform ongoing due diligence before contract renewals, if you notice performance issues, or if there are new or updated regulatory requirements.

venminder

Risk & Performance Monitoring

Between formal risk re-assessments and due diligence, it's necessary to constantly monitor for new or emerging risks, ensure the vendor's performance is as expected, and that the value of the relationship outweighs the risks. To do this:

→ Stay on top of negative vendor news, industry or regulatory changes, or other risk indicators. Using subscription-based vendor risk monitoring and alert services can be helpful.

→ Hold regular performance reviews with your third party to formally discuss performance, review SLAs and KPIs, and identify any issues before they become major problems.

→ Consider whether the third party's cost/risk-to-benefit ratio has changed enough to consider ending the relationship and whether the third party has met its contractual obligations.

Contract Renewals

Review your contract at the midpoint of the contract term to determine if changes are necessary before renewal. In addition to your standard contract terms, consider including the following:

→ Provisions such as regulatory compliance requirements, breach notification requirements, software service levels, exit strategies for both planned and unplanned terminations, and a right-to-audit clause.

Offboarding

Projects end, vendors perform poorly, or your organization needs to move on to other vendors offering different products, services, or costs. No matter why you end the relationship, following the steps in the offboarding stage is essential:

Termination

Notify your third party that you've decided to terminate the contract:

→ Make sure you read and understand the termination requirements in the contract, including notification of termination timing and any costs associated with ending the contract early.

→ Remember that the relationship hasn't concluded until the contract's expiration date.

Exit Plan Execution

Review and follow your organization's detailed exit plan that covers the various tasks and responsibilities that need to be carried out before, during, and after contract termination. Keep the following in mind:

→ You must ensure that your third party returns or destroys sensitive data and that your organization has a process for revoking access to your networks, information, and facilities.

TPRM Closure

Tie up loose ends and handle the final task of closing the relationship. Don't forget to do the following:

→ Update the vendor's status in all systems, including your third-party risk management and Accounts Payable systems.

→ Archive all relevant information and documents just in case you need to access it for an audit or exam.

Third-Party Risk Management Roles and Responsibilities

External Audtiors and Examiners

Responsibilities include monitoring compliance with laws and regulations, reviewing policies, records, and governance documents, identifying violations, and recommending corrective action. Regulatory examiners represent a specific regulatory agency and conduct audits to confirm compliance with regulatory requirements and guidelines within their jurisdiction.

Board of Directors

Ensures that senior management and the organization execute third-party risk management activities effectively and within the acceptable risk tolerance. They set the tone-from-the-top by emphasizing the importance of third-party risk management and holding senior management accountable. They approve the TPRM policy and regularly review the program's progress and effectiveness.

Internal Audit

Their primary role is to ensure that the TPRM program and processes operate effectively, comply with all laws and regulations, and hold all stakeholders accountable.

Senior Management

Along with the board of directors, they ensure that third-party risk management is a priority within the organization. They hold stakeholders accountable for fulfilling their roles and responsibilities, review and approve the policy, address concerns, provide necessary resources, and determine if the risks present in the third-party portfolio are acceptable.

Third-Party Risk Management Team

This individual or team is responsible for the third-party risk management framework, which incorporates all the requirements, rules, tools, and processes necessary to effectively execute TPRM within the organization. They're responsible for the TPRM policy, system, workflows, and documentation as well as ensuring that TPRM processes are executed correctly and in sequence. Issue management, escalation, and reporting are also key responsibilities.

Subject Matter Experts

These individuals can be internal or external and are responsible for conducting the formal review and assessment of a vendor's risk management practices and evidence of their controls as part of due diligence. Subject matter experts should have professional certifications or credentials in their specific risk domain.

Lines of Business

The lines of business are responsible for identifying and engaging potential third parties and managing those third parties, per the requirements of the TPRM program, throughout the relationship.

Third Party Owner (Vendor Owner)

Within the line of business, these individuals are specifically appointed to manage the relationship with the third party per TPRM rules and requirements. Third-party owners also own the risk associated with the relationship. They're responsible for completing all necessary TPRM activities on time and at the expected level of quality. In addition to completing inherent risk assessments, they ensure the vendor provides requested data during due diligence, remediate issues, negotiate contracts, and manage the third party's risk and performance.

Third Party or Vendor

Third parties are responsible for providing products and services to your organization or its customers. They must abide by your organization's TPRM requirements, provide high-quality products and services, and follow your relationship's contractual terms and conditions. They also must manage their third parties (your organization's fourth parties) in a manner consistent with your organization's expectations and requirements.

Fourth or Nth Parties

These are the business entities that work directly for your third parties. Your organization has no direct relationship or business agreement with these organizations. However, the products or services they provide to your third parties can directly or indirectly impact your business.

venminder

Who's Ultimately Responsible for Overseeing Third-Party Risk Management?

Third-party risk management is a complex process that requires the participation of many different stakeholders. However, at the end of the day, your board of directors and senior management oversee your third-party risk management program and ensure that third-party risk management activities are executed effectively.

venminder

Putting It All Together – Third-Party Risk Management Program Essentials

Know Your Regulations

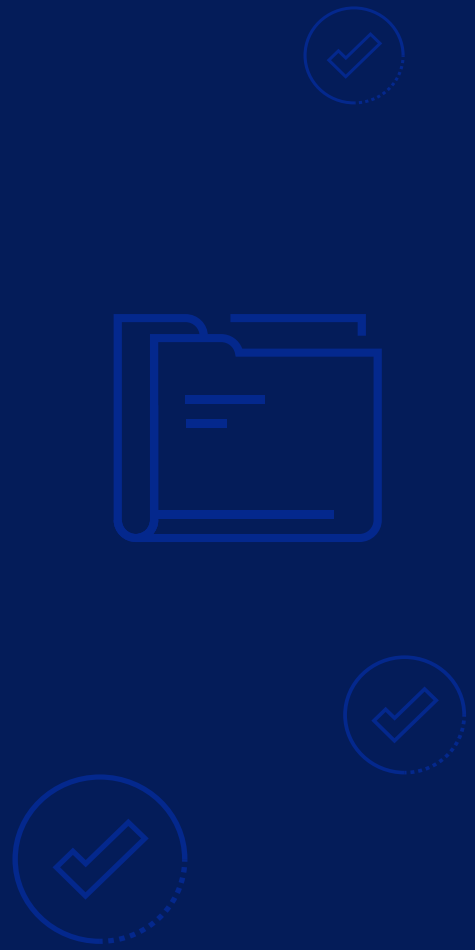
Suppose your organization is in a regulated industry. In that case, you must understand the regulatory requirements and expectations for third-party risk management. Take time to learn these regulations, read the guidance, and determine how your organization will comply.

Identify Your Third Parties

It's important to identify all individuals or organizations that provide products or services to your organization (or its customers) or with whom you have business relationships, such as referrals or profit-sharing agreements. Your Accounts Payable department can help you identify any business entity paid by your organization. Make sure you identify what product or service each third party provides to the organization.

Define the Scope of Your Third-Party Risk Management Program

You must determine the product or service types to include within your program scope. Most product and service types should qualify for third-party risk management. However, not all third parties will be in scope for your program. For example, public utilities, sponsorships and donations, industry memberships and conferences, and magazine subscriptions are typically excluded from third-party risk management programs. Remember, it's up to you and your organization to determine your third-party risk management program scope. Just be sure you can articulate and defend your decisions to exclude specific product or services types.



venminder

Develop the Methodology to Risk Rate Each Vendor Engagement

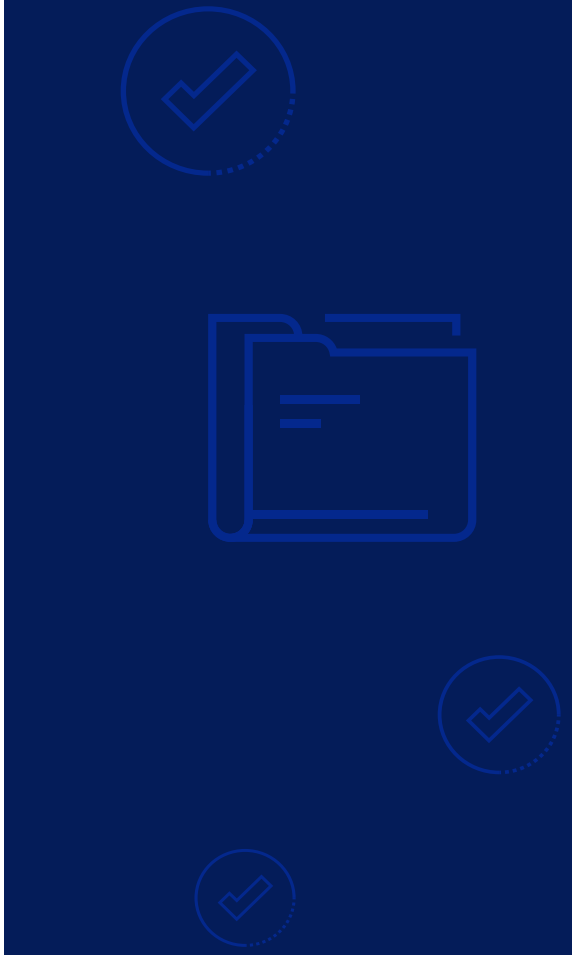
Every third-party engagement (each product and service) should have a risk rating, which also becomes the risk rating for the relationship. Your organization must identify and document how risk ratings are calculated. As a best practice, risk rating scales are limited to low, moderate, and high-risk ratings. For third parties that provide multiple products or services, the third-party risk rating should reflect the rating of the highest risk engagement. For example, a third party may sell your organization three different products or services. Two services are considered low risk, while the third is rated high risk. In this case, the third party would automatically be rated as high risk.

Identify Critical Vendor Criteria

In addition to identifying the risk level of each third-party engagement, you must identify which third parties are critical to your operations. Critical third parties are those who, should they fail or have an unplanned and prolonged outage, would prohibit your organization from conducting business as usual or even at all. Three basic questions can help you determine if a vendor is critical:

1. Would a sudden loss of this vendor cause significant disruption to operations?
2. Would that disruption impact your customers?
3. If the time for the third party to recover operations exceeded 24 hours, would there be a negative impact on your organization?

If you answer yes to any of those questions, you're probably dealing with a critical third party. Remember that critical is NOT a risk rating, but a label indicating those third-party relationships most important to your operations. A vendor might be high risk and critical to your operations, but not all high-risk vendors are critical.



Identify Stakeholder Roles and Responsibilities

Successful execution of third-party risk management requires the participation of multiple stakeholders. Establish the roles and responsibilities for your subject matter experts, third-party owners, the third-party risk management team, and other stakeholders. There must also be a a documented third party or vendor owner for each third-party engagement within the program's scope.

Build Workflows That Follow the Third-Party Risk Management Lifecycle

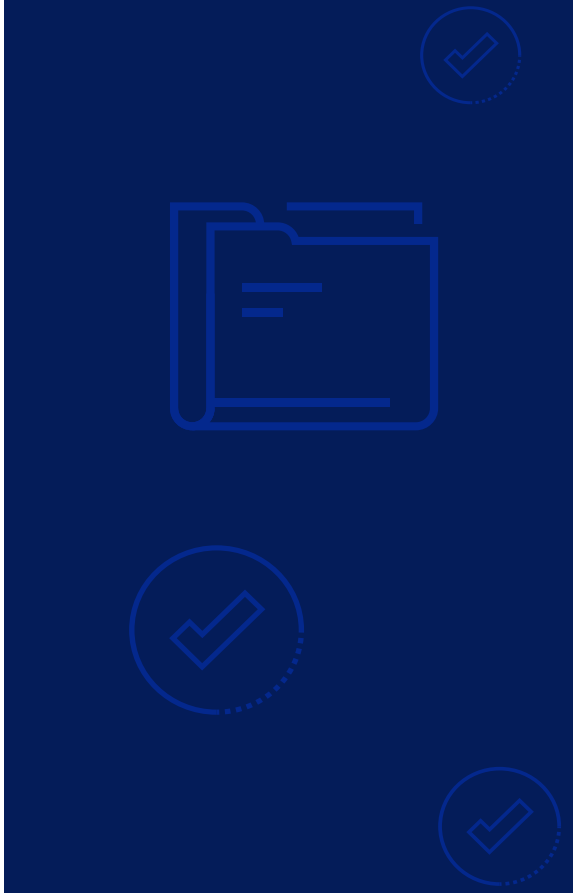
The third-party risk management lifecycle was designed to ensure the right activities are completed at the right time and in the right sequence. Designing your workflows to follow the lifecycle will ensure you complete all the necessary steps within each stage of the lifecycle.

Establish and Formalize Governance Documents

- → **The policy** is a high-level document that describes the rules and requirements for your organization's third-party risk management program. It outlines the structure and concepts of your framework, stakeholder responsibilities, and guidelines for specific processes. It should be reviewed and approved by senior management and the board of directors annually.

- → **The program** informs senior management, the business lines, and other stakeholders what is necessary to maintain an effective third-party risk management program. It details the processes, workflows, stakeholder activities, and timing needed to meet policy requirements.

- → **The procedures** provide step-by-step, detailed guidance for executing the processes detailed in the program document.



Establish Third-Party Risk Management Reporting and Routines

Reporting is a key element of effective third-party risk management programs. Board and senior-level management reports are essential for validating the effectiveness of your program and enabling them to drive action and make decisions. Other must-have reports include a critical vendor inventory, issue management, and reports detailing the timing and progress of due diligence risk assessments and re-assessments. You can develop additional reporting for various purposes and stakeholder groups as your program progresses.

Strive for Continuous Improvement

Third-party risk management programs aren't meant to be static. As time progresses, regulations and risks will change and evolve, and your program will need to be updated. Make sure you objectively review your program at least once a year to identify any gaps or weaknesses and create improvement plans.

venminder

Consider Tools to Help You Facilitate Third-Party Risk Management

Implementing and maintaining an effective third-party risk management program can be overwhelming with limited resources or expertise. However, there are numerous third-party risk management technology and service solutions out there that can support and supplement any program.

Today's third-party risks are too numerous and complicated to manage with manual processes and spreadsheets. Not only are manual processes inefficient, but they're also extremely error-prone. Your program's efficiency can be improved by using third-party risk management software to standardize workflows, automate key processes, and organize documents.

Depending on your situation, you might also consider outsourcing some of your third-party risk management activities to a qualified third-party risk management firm. For example, collecting due diligence documentation can be very time-consuming, but adds little value. Outsourcing the collection of those documents can give your third-party risk management team valuable bandwidth to focus on activities that identify and mitigate risk. Third-party risk management firms can also provide you with professional and credentialed subject matter experts to perform vendor risk assessments.

Even though third-party risk management is a complex practice with many interdependent processes and stakeholders, it doesn't have to be overwhelming and impossible.

Identifying third-party risk management requirements and best practices for your industry, and following the third-party risk management lifecycle, are excellent building blocks when implementing third-party risk management programs.

From there, a step-wise approach can help you create processes, workflows, documentation, and reporting for a comprehensive and effective program.

Don't forget to work smart! Consider how technology and external third-party risk management services can add bandwidth and improve the quality, efficiency, effectiveness, and even the cycle time of your processes, too.

Download samples of vendor Control Assessments
and see how Venminder can help reduce your third-party risk management workload.

Download Now

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise, and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting, and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals, and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance, and more.