A Business Case for

Third-Party Risk Management

venminder

venminder

Table of
Contents

A Business Case for
Third-Party Risk Management

In recent years, there's been a growing need to address third-party risk, which impacts organizations across all industries. Organizations are increasingly outsourcing products and services to gain a competitive advantage, obtain access to specific expertise, supplement their capabilities, or better serve their customers. Third parties are often essential to provide certain products and services, but they can also expose organizations to risky situations like data breaches, regulatory noncompliance, reputation damage, operational disruptions, and more.

> *Research from Gartner has shown 61% of organizations in the U.S. have been directly impacted by software supply chain attacks in the course of a year. Other research shows 66% of consumers say they wouldn't trust an organization after a data breach. Now, more than ever, it's extremely important to gain visibility across the entire supply chain and evaluate the risks third and fourth parties pose.*

Certain industries, like financial services and healthcare, have traditionally managed these risks through the business practice known as third-party risk management (TPRM), also referred to as vendor risk management (VRM). However, it's becoming increasingly evident that all organizations can benefit from identifying and managing third-party risks.

TPRM is often mistaken for a basic check-the-box activity, which undervalues its importance. In reality, TPRM is a highly rewarding practice for an organization and its stakeholders. Various departments and stakeholders need to play a role in managing third-party relationships, but it can be challenging to understand the true value this practice can bring.

This eBook provides a business case for TPRM and explores why your organization should invest in this essential business practice.

venminder

An Overview of TPRM

What TPRM Is

Third-party risk management (TPRM) is the systematic approach to identifying, mitigating, and managing risks that occur in third-party business relationships. Take a moment and consider some of the third parties or vendors that engage with your organization. You can likely think of several that provide essential products and services, such as IT support, payroll, marketing automation, cloud services, and more.

Now, consider some of the risks that exist when working with these third parties. How might your organization be affected if your IT support vendor were to suddenly shut down or your cloud service provider suffered a data breach? TPRM helps identify and mitigate these risks, so your organization and customers are better protected in those situations.

Here are some of the key third-party risks and how they can impact your organization:

1. ## Compliance risk
   A third party fails to comply with laws and regulations that govern the products and services your organization provides to customers. This can lead to regulatory fines, lawsuits, and reputational damage, even if the third party is at fault.

2. ## Operational risk
   A third party is unable to conduct business as usual due to either an internal or external disruptive event. This can lead to disruptions in the services your organization provides to customers, potentially causing reputational damage, lost business, or even regulatory fines.

3. ## Reputation risk
   A third party negatively impacts your reputation due to adverse events like data breaches, poor services, or lawsuits. Customers may begin to distrust your brand, or your organization may be the subject of negative news coverage as a result.

4. ## Information security and cyber risk
   A third party lacks proper security controls or mishandles your data. This puts your customers' information at risk for data breaches, cyberattacks, and other security incidents.

5

Strategic risk

A third party's actions or decisions don't align with your organization's objectives. If a third party doesn't have a shared understanding of your objectives, this can lead to poor services and performance.

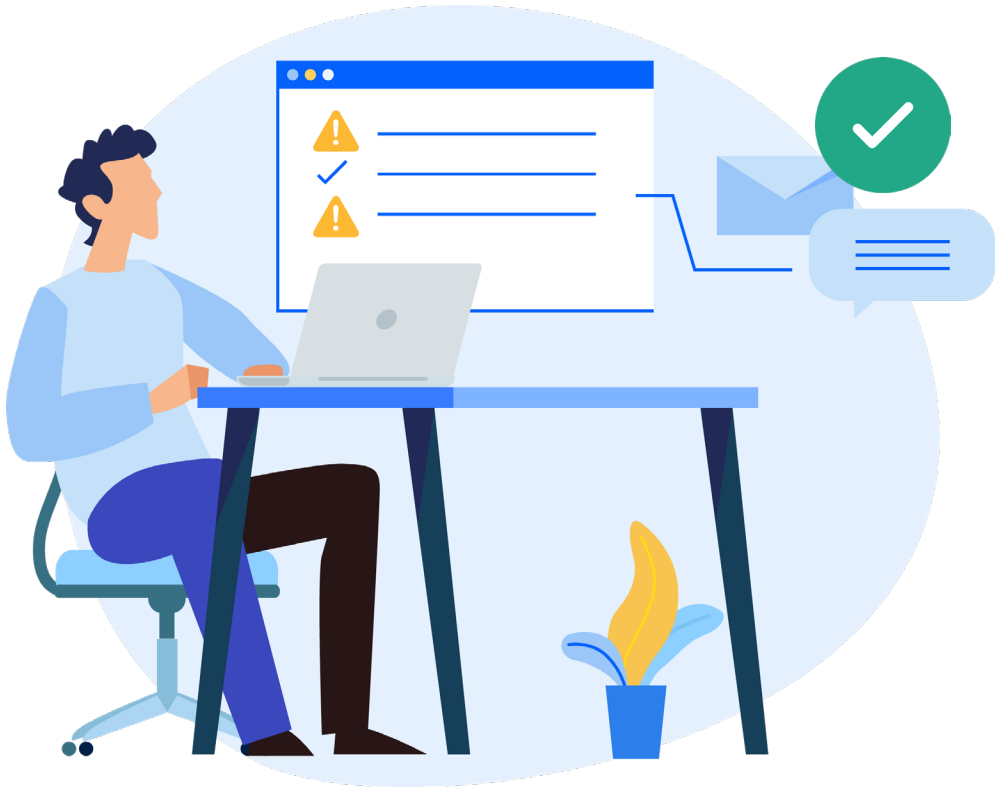
6

Financial and credit risk

A third party has poor financial health and is unable to retain qualified staff, invest in effective technology and programs, and provide quality products and services. As a result, the third party is unable to meet expectations or may even go out of business altogether.

Some of these risks may overlap, so it's important to address all third-party risks as any of these can negatively impact your organization. Depending on your organization or industry, third parties may pose other risks like concentration risk or geopolitical risk.

Ultimately, TPRM helps identify and manage these risks so your organization can engage with its third parties safely and soundly. Additionally, TPRM provides value-added benefits for departments across an organization that also makes the investment worthwhile.



Why TPRM Is Important

Third-party risks continue to grow and evolve year after year. Global conflicts, economic sanctions, and climate-related events are disrupting supply chains across the world and increasing the potential for financial loss in many organizations. The ongoing risk of third-party data breaches can also impact an organization's financials through the high costs of legal fees, fines, settlements, and lost revenue.

Investing in TPRM helps organizations be better prepared to respond to these events, and can help minimize operational disruptions and expenses. As your organization continues to outsource products and services, TPRM helps fully realize the benefits of outsourced relationships. Effective TPRM practices like risk assessments, due diligence, and ongoing monitoring help ensure third parties perform as expected and deliver the anticipated value to your organization.

While TPRM protects your organization and customers from third-party risks, it can also enhance your overall business strategy. TPRM activities like vendor selection, contract management, and ongoing monitoring are strategic processes that can help save costs and maximize the value of your relationships. When your organization implements a practice to mitigate third-party risks, manage third-party issues, and monitor third-party performance, the benefits can extend through the entire organization.

The Organizational Value of TPRM

For those unfamiliar with TPRM, it may help to consider how this practice can provide organizational value and a return on investment (ROI). Implementing a TPRM program may require investing additional time and resources initially, but it can provide significant benefits across an organization. As your TPRM program matures and grows, the value added for each department also increases. While TPRM manages third-party risks like the ones outlined above, it also provides other strategic objectives that can grow and sustain your business.

Benefits and ROI of TPRM for Each Department

Benefits of TPRM for Finance

Third-party risk management (TPRM) can be a significant financial investment, depending on the additional resources, tools, and staff that are needed. It's understandable that the finance department may be hesitant about implementing this practice without a deeper understanding of its value.

3 TPRM Benefits for Finance:

Drives enterprise and strategic value creation.

Third-party relationships drive value for departments and teams that create revenue growth, operational efficiencies, and cost savings. TPRM provides visibility into the full third-party inventory and the nature of those third-party relationships. This gives finance teams a thorough understanding of the value these third parties can create for your organization. This value can be effectively communicated to key internal and external stakeholders, including your team members, board of directors, and investors to show how TPRM can drive meaningful enterprise value creation for your business over a short and long-term horizon.

BY THE NUMBERS

A study from Deloitte found that only 13% of respondents have a fully mapped supply chain network and 72% have partial or limited visibility. This puts organizations at risk of unexpected financial losses when disruptions happen.

Reduces budget surprises and minimizes financial exposure.

Getting a comprehensive view of your third-party vendor base and the risks that exist within the third-party relationships helps avoid financial and budget surprises and reduce financial exposure your organization may face. The finance department's daily workflow includes managing revenue growth and costs across the organization but can be further contextualized and improved with a TPRM program, toolset, and processes in place. At the end of the day, no one likes spending over budget and exposing the organization to unplanned financial expenses, so finance teams should ensure TPRM is in place across every team to help reduce the impact of budget surprises and misses.

Ensures third parties provide anticipated value to your organization.

Are the third parties actually helping you address a problem or realize an opportunity? TPRM provides the structure to review and evaluate expected third-party performance to verify that service level agreements (SLAs) are being met. Proper management of third-party performance helps protect your budget dollars and revenue.

The ROI for Finance

Effective third-party relationships are often a key factor in driving operational efficiencies, increasing revenue, and reducing costs. TPRM can help you realize cost savings by identifying third parties that may not be adding the expected value or are providing duplicate services. A TPRM program provides finance teams with the audit trail, documentation, and information needed to have confidence in meeting and exceeding budget targets and reducing financial exposure and costs.

Benefits of TPRM for Legal

A properly drafted third-party contract is a crucial factor in managing third-party risks, and the legal department needs to be actively involved in this process.

Initially, TPRM might seem like a challenging task, which demands extra effort. Nonetheless, the proactive approach of TPRM can save the legal team thousands of hours by preventing potential issues instead of responding reactively to them.

2 TPRM Benefits for Legal:

Supports consistent contract management.

TPRM can be beneficial for legal teams, as it helps them manage third-party contracts more effectively. By implementing a consistent process for planning, negotiating, executing, storing, and managing legal documents, TPRM can reduce errors and increase efficiency. An effective TPRM program assigns responsibilities and sets reminders for important dates and contract reviews, thereby lessening the burden on legal teams. This enables them to focus on their core competencies and strategic objectives while TPRM helps manage the administrative details for contracts.

Helps monitor third-party performance.

Third parties that are failing to deliver products or services as expected can expose your organization to various risks like reputational harm or noncompliance. TPRM gathers important information to help keep legal teams informed of a third party's performance and help identify any unmet service level agreements (SLAs). This allows the legal team to reassess the third-party contract and make decisions about renewal or termination.

The ROI for Legal

Effective TPRM can benefit legal teams in many ways. Investing in TPRM gives your legal team better insight into third-party contracts and performance, which ultimately helps reveal the overall value of your third-party relationships. By implementing robust TPRM measures, organizations can minimize legal exposure to third-party risks and potential lawsuits. This can save your organization significant legal costs and resources, allowing legal teams to focus on more strategic initiatives that benefit the business.

Benefits of TPRM for Operations

Many organizations have a wide network of third parties they partner with, which can create a unique set of challenges for an operations team. Instead of treating TPRM as a separate function, an operations team should consider ways to integrate it into their existing processes.

3 TPRM Benefits for Operations:

Improve risk intelligence.

An organization's risk landscape expands across multiple domains, which creates additional challenges when those risks are evolving. TPRM offers an effective solution to continuously monitor and manage new and emerging third-party risks. As risk intelligence improves, organizations can make informed decisions about strategic goals.

Strengthen compliance efforts.

Compliance teams are familiar with the many challenges of keeping organizations in compliance with regulatory expectations, laws, and industry standards. Implementing a TPRM program can help support these compliance efforts by ensuring an organization's third parties are following the same guidelines. Some regulations are listed here.

Build operational resiliency.

Although business-disrupting events can't be fully avoided, it's important to have a strategy in place that minimizes the impact. This strategy should not only contain the internal processes of your organization, but also those of your third parties. TPRM helps build operational resiliency by identifying third parties that are most significant to your organization and evaluating their preparedness response strategy for business interruptions.

BY THE NUMBERS

Research from Gartner revealed that up to 45% of organizations have experienced a business disruption because of a third party. These disruptions can delay or shut down services for customers, damage reputations, and ultimately increase costs and decrease revenue.

The ROI for Operations

TPRM identifies third parties that are considered critical to your operations, so your time and efforts are spent where they're needed most. By mitigating the risks of operational disruptions, organizations can save money in the long run and achieve a higher ROI in technology and innovation.

Benefits of TPRM for Cybersecurity and Information Security

Protecting data from breaches, cyberattacks, and other security incidents will continue to be a challenging business priority. A TPRM program with robust cybersecurity procedures can help ease these challenges for cybersecurity and information security teams.

2 TPRM Benefits for Cybersecurity and Information Security:

Safeguard and protect customer data.

TPRM provides immense value to teams tasked with protecting an organization's data. These teams must be especially vigilant to ensure third parties have effective controls in place to protect customer data against cyberattacks and security breaches. Many TPRM activities like risk assessments, due diligence, and ongoing monitoring will support cybersecurity and information security teams by providing better visibility into a vendor's security posture.

As more privacy regulations are passed and expanded across the globe, data protection is also becoming a key focus. Since many third parties store, transfer, or access sensitive data, organizations are expected to ensure this data remains secure.

Help identify poor cybersecurity practices.

A third party with ineffective or non-existent cybersecurity practices puts your organization and customers at risk of data breaches, ransomware attacks, and more. TPRM helps identify these risks early on, which can assist in the third-party selection process, and then monitor for changes on an ongoing basis.

BY THE NUMBERS

Only 13% of organizations continuously monitor third-party security risks, according to a study from Panorays. This leaves organizations at risk of third-party data breaches, reputation damage, and financial repercussions.

The ROI for Cybersecurity and Information Security

Investing in TPRM can yield significant ROI when it comes to cybersecurity and information protection. The global average cost of a data breach is a staggering $4.45 million, which can have devastating effects on your organization as well as the third parties involved. Identifying and mitigating third-party cybersecurity risk proactively is a vital strategy that helps avoid costly financial consequences such as legal fees, settlements, and irreparable harm to your reputation.

Benefits of TPRM for Marketing and Sales

TPRM offers a lot of value to other departments but may seem less relevant to the objectives of marketing and sales.

3 TPRM Benefits for Marketing and Sales:

Uncovers new business opportunities.

TPRM creates opportunities to safely engage with third parties that may have unique or innovative products and services. These engagements can ultimately lead to strong partnerships, which allows your organization to deliver high-quality products and services to your customers.

Creates a competitive advantage.

Customers are often more willing to work with an organization that has TPRM practices in place, especially as it relates to protecting their data. By maintaining a reputation for effectively managing risks, an organization can attract new customers and retain existing ones, ultimately leading to increased sales and revenue.

Protects your reputation.

Some of your third parties may provide products or services on your behalf, which essentially means they represent your organization. In these situations, your reputation is significantly impacted by your third parties' actions, both good and bad. TPRM activities like performance monitoring help ensure you identify and remediate any issues before they become larger problems that harm your reputation.

The ROI for Marketing and Sales

Effective TPRM can provide organizations with a significant sales advantage. Customers are becoming increasingly concerned with data security and privacy and are more likely to choose a company that demonstrates a strong commitment to protecting their sensitive information. By implementing robust TPRM measures, organizations can assure customers that their data is safe and secure, which builds trust and confidence in the brand. This can result in increased sales and customer loyalty, as well as a competitive advantage over organizations that neglect to invest in TPRM.

Overall ROI of TPRM

ROI of TPRM

Not only does third-party risk management (TPRM) produce an ROI for individual departments across organizations, but it also has overall returns that benefit the entire business.

4 Examples That Reveal ROI of TPRM:

Removes duplicative services and shadow purchasing – TPRM helps prevent organizations from operating in silos and can provide cost savings on services and products that are duplicated across departments. TPRM can also help prevent departments from purchasing third-party services or products without proper due diligence and contract negotiations.

Helps avoid regulatory and legal fines – Some industries, like financial services, have extremely prescriptive guidance on TPRM that can lead to steep regulatory fines and legal costs. But if you aren't in the financial industry, you're still at risk of regulatory scrutiny. Regulations like the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and multiple state privacy laws have expectations for how third parties handle things like protected health information (PHI), consumer data, and data privacy.

Minimizes negative impact from the loss of third parties – It's essential to plan for the loss of a third party, which may have been anticipated because of a contract expiration or unexpected because of a sudden decline in the third party's performance or financial health. A TPRM program puts plans and contractual standards in place that help ensure your organization can continue operations with minimal disruptions as you end a third-party relationship.

Protects your reputation – Unfortunately, if a third party performs poorly or suffers a breach that impacts your customers, the consequences often land on your organization. Even adverse media about your vendor can reflect poorly on your brand. With TPRM, third parties are regularly managed and monitored for performance, risk, and negative news, minimizing the chance of significant issues that could harm your reputation and brand.

Tips to Calculate the ROI of TPRM

ROI calculations for TPRM will primarily focus on cost avoidance, so it's important to set the right expectations in your business case. Be creative in calculating how your organization will benefit from the investment of time and resources needed for TPRM.

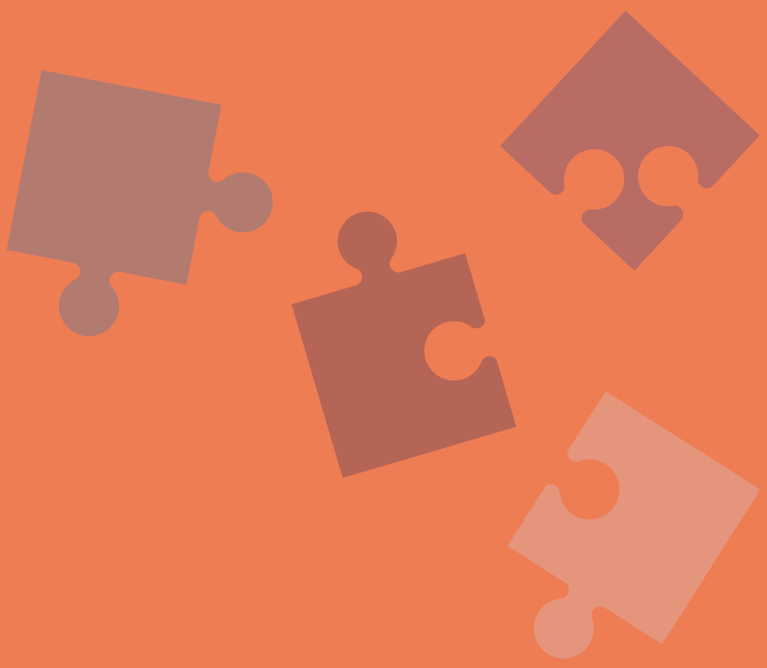
Here are some tips to keep in mind as you calculate the ROI of TPRM:

Use relevant data – You may be limited to the type of data you can find to support your business case. For example, your finance department might be unwilling or unable to provide data about the value of your customers. In these situations, consider using datasets that represent the average for your organization's size or industry.

Determine the long-term impact – It's important to consider the long-term impact of a single incident represented in your ROI calculation. For instance, while your initial ROI calculation might consider the potential cost of breach remediation and the associated legal fees, it's also crucial to recognize that an incident often has further long-term effects, such as the loss of customer trust and revenue and damage to your reputation and brand.

Supplement with real-world examples – ROI calculations can be more impactful if you can supplement them with real-world examples. Regulatory fines and penalties related to third-party data breaches can be especially helpful and are usually easy to find online.

Building a Business Case for TPRM



Process Example for Building a Business Case for TPRM

The process and duration of building a third-party risk management (TPRM) business case will look different for every organization depending on existing resources and capabilities.

Here's an example of what that building process may look like:

Learn the basics.
It's important to understand some of the core concepts of TPRM and why this practice is so important. This will help you draft and communicate your business case with confidence.

Do your research.
Make sure you have a general understanding of any TPRM regulations that are applicable to your industry, as well as the potential consequences for noncompliance.

Collaborate with other stakeholders.
You may have a limited view of some of your organization's challenges or business strategies, so it helps to collaborate across different departments and collect more information for your case.

Outline and draft your business case.
Consider the information you'll include in your business case, such as the problems you've identified and how they can be solved with a TPRM program. You'll also want to include calculations that show the ROI of TPRM.

Get a peer review.
Whether you created the business case independently or with a group, it's worthwhile to ask for a peer review. This can help identify any areas that might be unclear or underdeveloped.

Present your business case.
The method in which you present your business case should depend on your audience. An informal, one-on-one meeting might be preferable to some, while others might expect a formal presentation.

How to Create and Present a Business Case for TPRM

Maybe you understand the need for TPRM at your organization, but now you have the task of getting other stakeholders like senior management, department leaders, and the board of directors on board. This can be challenging, but it's not impossible! A business case can help lay out the need for TPRM and the solution for your organization. Your specific business case may differ depending on the audience you're presenting to.

Here are some tips for creating and presenting a business case for TPRM:

Lay out the problem.

It's important to make sure that your organization understands the reasons why it needs to invest in TPRM and outline the program accordingly. Perhaps your organization has been recently affected by a third-party data breach, or your operations are being disrupted due to a third party's poor performance. It's crucial to be clear on why TPRM is a valuable investment and communicate it effectively to everyone involved.

Emphasize the value and benefits of TPRM.

Once you've identified the problem, don't leave it unresolved! Describe how TPRM can provide a solution and how it will benefit both the organization as a whole and individual departments. It's important to understand each stakeholder's perspective and hesitations. Take time to understand their knowledge, questions, and concerns about TPRM.

Support your claim with research, numbers, and facts.

It's one thing to present the problem and solution, but it should be backed up with hard evidence. Using studies on TPRM, like third-party data breach numbers and costs or supply chain disruption statistics, are helpful to include throughout. There are also organization-specific numbers like the size of your third-party inventory, the number of critical and high-risk third parties, and time spent onboarding third-party vendors.

Include a financial analysis.

It's a good practice to outline what the investment into TPRM will look like, including staffing, the costs of any additional tools like software, and time needed to perform tasks effectively. Also consider including potential ROIs using actual data from your organization. This can make your financial analysis more impactful and the business case more influential.

Consider the formatting and presentation.

A business case can be formatted and presented in a variety of ways, so consider what works best for your organization and stakeholders. You may want to include helpful visuals like graphs or charts to display your data and it's important to be mindful of the length, so your audience isn't overwhelmed with information. Whether you choose a PowerPoint presentation or a simple Word document, your business case should be clearly formatted and easy to follow.

Create an implementation plan.

Your business case will likely be better received if you include an implementation plan with roles, responsibilities, and timelines. This can give stakeholders realistic expectations about the potential challenges you may face when implementing TPRM. It can also give reassurance about how your organization can use any existing resources for your TPRM program.

Successfully Implementing TPRM

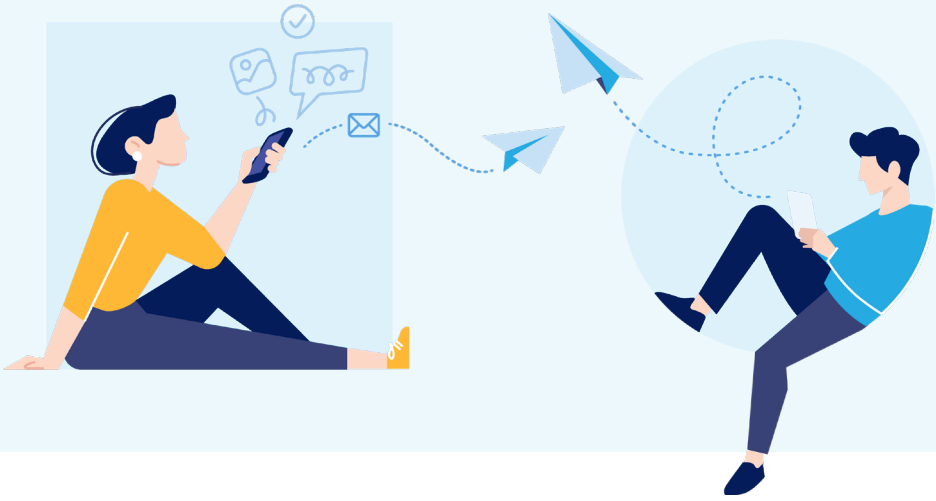
Tips for Successful Implementation of TPRM

Now that you understand some of the value third-party risk management (TPRM) can bring to your organization, it's important to successfully implement this practice. A TPRM program that can grow and scale with your organization will ultimately offer the most value. The timeline and ease of implementation may depend on different factors such as your organization's size and industry, availability of staff, number of third parties, and budget.

Here are some general tips that will help get you started:

Get leadership buy-in – Senior management and the board of directors should understand the value of TPRM so they can advocate for this new business activity throughout the organization. Their support and guidance are essential for ensuring your TPRM program is aligned with your organization's strategic goals and objectives.

Keep in Mind:
Obtaining buy-in from leadership can be a daunting task! As a starting point, begin talking to department leaders to hear and understand their concerns or hesitations. This can help you tailor your business case and ensure concerns are addressed.



Establish a policy – A TPRM policy document should outline certain details of your program such as the scope, minimum requirements, and non-negotiable rules. The policy should also define roles and responsibilities and broad guidelines for specific processes, though not step-by-step procedures. Senior management and the board should review and approve the policy at least annually.

Why do you need a policy?

A TPRM policy is essential to communicate rules, requirements, and guidelines throughout an organization. This document is a regulatory requirement for many organizations and lays the foundation of your overall TPRM framework and program.

Creating a policy for your TPRM program will take some collaborative effort, but here are some steps to get you started:

> **Review regulatory requirements.** If you're in a regulated industry, it's important to review any applicable guidance related to your policy. You don't want to spend time and effort writing a policy only to discover it doesn't align with regulatory guidance.

> **Confirm internal expectations and requirements.** Consider whether your organization uses a specific policy format or template so you can use this as a starting point. You should also confirm who will be the policy owner and how the policy will be reviewed, approved, and enforced.

> **Define key details.** Make sure you understand the purpose of the policy and can identify the users and process stakeholders. It also helps to consider the definitions of terms that will be used throughout the policy. Defining these details early in the process can help avoid time-consuming revisions.

Create a third-party inventory – Work with your Accounts Payable department to build a list of third parties that are paid by your organization. These will generally include third parties that provide products and services directly to your organization or to its customers. It's also important to identify which product or service the third party provides. This process will give you a good starting point so you can then determine the scope of your TPRM program, as not every third party will need to be included.

Define the scope – The scope of your TPRM program is essentially the definition of what types of products or services will need to be managed. Most third-party products and services should be included in your TPRM program, but there may be some exceptions. Public utilities are generally exempt because there are no other alternatives in the market. Sponsorships, donations, industry memberships, and magazine subscriptions are other examples that usually don't need to go through the process of TPRM. Your organization must make this determination for itself and be able to articulate and defend your reasoning to exclude certain product and service types.

The business case for TPRM varies for each organization and department. Depending on your current goals and challenges, certain value-added benefits may be more relevant than others. Nevertheless, the crucial point is that TPRM can provide significant organizational value.

Calculating the ROI can help bring clarity to the benefits of this essential business practice.

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

Download Now

Sources

- **Gartner.** (October 21, 2023). Mitigate Enterprise Software Supply Chain Security Risks. https://www.reversinglabs.com/gartner-report-mitigate-enterprise-software-supply-chain-security-risks
- **Vercara.** (December 18, 2023). Vercara Research: 75% of U.S. Consumers Would Stop Purchasing from a Brand if it Suffered a Cyber Incident. https://vercara.com/news/vercara-research-75-of-u-s-consumers-would-stop-purchasing-from-a-brand-if-it-suffered-a-cyber-incident
- **IBM.** (2023). Cost of a Data Breach Report 2023. IBM. https://www.ibm.com/reports/data-breach
- **Deloitte.** (October 2022). Procurement and supply chain resilience in the face of global disruption. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consultancy/deloitte-uk-procurement-and-supply-chain-resilience.pdf
- **Gartner.** (December 13, 2023). Gartner Survey Finds 45% of Organizations Experienced Third Party-Related Business Interruptions During the Past Two Years. https://www.gartner.com/en/newsroom/press-releases/2023-12-13-gartner-survey-finds-45-percent-of-organizations-experienced-third-party-related-business-interruptions-during-the-past-two-years
- **Panorays.** (2023). Navigating Third-Party Security Risks in 2023. https://panorays.com/resources/guides/third-party-security-risks/

venminder

+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.