venminder

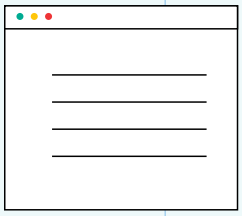
How to

Get Organizational Buy-In and Commitment for Third-Party Risk Management

Third-party risk management (TPRM) is a highly collaborative practice, but it's not uncommon for a small team or individual to be the driving force behind all the various activities. With so much to accomplish, there is often a need to invest in more resources, but it can be challenging to gain support from different stakeholders who may not share the same goals.

This resource will help you by providing five tips to follow when seeking buy-in.

It's easy to assume that everyone understands why organizations need TPRM. One might think it's enough to emphasize that TPRM is a regulatory requirement or a best practice. Still, that rationale may not be enough for everyone. Stakeholders may default to simply "checking the box" to fulfill minimum requirements, but a healthy and effective TPRM program requires an understanding of its purpose and value, as well as buy-in and support from the stakeholders.



Some of the stakeholders that may be supporting and/or participating in TPRM activities are:

- Upper management
- Subject matter experts (SMEs) across risk disciplines (business continuity, cybersecurity, financial, etc.)
- Vendor owners
- TPRM staff and governance
- Internal audit and accounts payable
- Legal

Each of these groups will approach TPRM from a different angle, so you'll generally want to highlight how their support of TPRM will offer organization-wide benefits. Let's explore how you can articulate the many requirements and benefits for your stakeholders to enhance their understanding and achieve their buy-in.

5 Tips to Follow If Seeking Stakeholder Buy-In for Your Third-Party Risk Management Program

01 | Focus on the benefits

Don't forget to emphasize the many benefits (beyond regulatory compliance) that TPRM offers, including:

Safeguarding information security and privacy

TPRM utilizes tools and processes to ensure that vendors with access to your organization's or customers' sensitive information have the necessary information security controls and practices to prevent cyberattacks and data loss, theft, or misuse.

> There's no way to predict if your organization will suffer a third-party data breach, but it's best to assume that one will happen eventually. Research from SecurityScorecard has shown that 98% of organizations have a vendor that's been breached in the previous two years. According to IBM and the Ponemon Institute, the global average cost of a data breach in 2023 was $4.45 million, a 15% increase over 3 years.

Protecting your operations

TPRM provides the framework to ensure vendors critical to your operations are appropriately vetted and have comprehensive business continuity and disaster recovery (BC/DR) planning and testing in place. TPRM identifies critical vendors, which triggers your internal BC resources to include them in their strategic planning.

> Third-party cyber incidents can also disrupt business operations, such as the case of a cyberattack on a car manufacturer's plastic supplier. The manufacturer was forced to stop production at 14 factories for one day, affecting around 13,000 vehicles.

Reducing financial loss

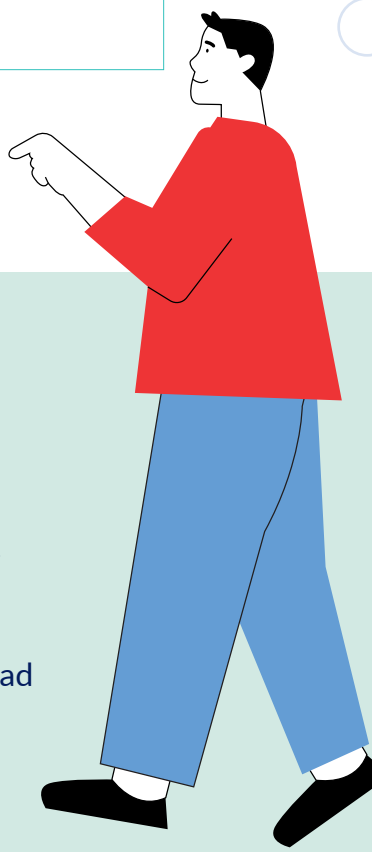
Regular third-party risk identification, assessment, management, and monitoring help protect your organization from costly regulatory fines, litigation, and poor vendor quality while improving overall business performance and increasing customer satisfaction.

> The SEC issued a multi-million-dollar penalty against a large financial institution for failing to protect its customers' sensitive data. The financial company had repeatedly hired a vendor with zero data destruction experience, which resulted in a breach that impacted approximately 15 million customers.

Defending your reputation and brand

Careful screening and monitoring of your vendors ensures your organization remains aware of any negative vendor actions or news (such as a data breaches, regulatory violations, or public relations issues) that could negatively impact your hard-earned reputation and brand.

> A marketing vendor that misled your customers about pricing would harm your organization in two significant ways. The first would be potential fines for Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) violations, and the second would be significant reputational harm from upset customers.



PRO TIP:

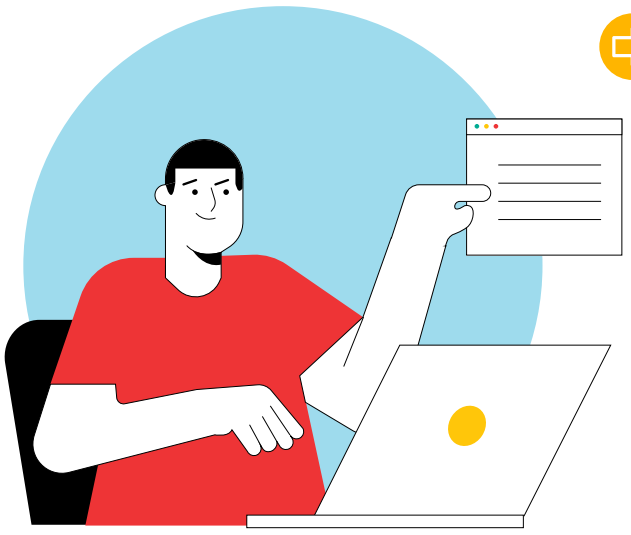
Know the relevant regulations

Being a regulatory requirement is an obvious reason, but one that is sometimes brushed off. So, you need to be prepared to explain it further. Ensure you know which regulations your organization needs to comply with and the potential consequences of non-compliance. These can include regulatory fines, litigation fees, and a damaged reputation from bad press. In severe situations, non-compliance can even result in suspended operations or imprisonment.

02 | Understand your stakeholder point of view

Every stakeholder will have a different experience and understanding of TPRM. For example, someone with a long history and background in financial services will better understand and appreciate the need for TPRM than someone from a non-regulated environment.

Not every stakeholder is going to automatically buy-in. So, taking time to learn about your stakeholders' knowledge, questions, challenges, and concerns about TPRM can help you tailor the best approach for gaining their support.



Potential Concerns and/or Misconceptions You May Hear and How You Can Respond

Vendor owners might be reluctant to engage in TPRM beyond the vendor selection stage.

After all, once the contract is signed, what else needs to be done? You may need to explain how ongoing monitoring, performance management, and periodic due diligence are important stages that can continuously validate the vendor relationship. These tasks can also be formally added to their role in terms of annual performance goals.

Upper management may question the need for maturing your TPRM program.

If you're struggling to obtain buy-in or additional resources to improve your program, try discussing the ways you can significantly improve your processes and satisfy your regulators who expect to see more than "good enough". You may also want to highlight the potential savings that TPRM can provide, whether it's avoiding disruptions, preventing your organization from contracting duplicative services, or ensuring you're getting the expected value from the vendor.

SMEs aren't always familiar with TPRM processes and might assume the workload will be an unnecessary burden.

This could be an opportunity to reassure these individuals that TPRM is not a solitary practice, and they'll continue to receive support and communication to ensure their success. Impress upon them that their skills are unique and necessary to complete thorough TPRM efforts. Consider speaking to their manager to ensure they have the bandwidth to support this and are rewarded as part of their employee performance.

03 Emphasize the dangers of not managing third-party risk

Failing to properly manage third-party risk can result in significant and long-lasting issues for your organization. Here are just a few of those issues you could face because of your third parties:

Data breaches

There is no shortage of news about massive data breaches involving a vendor or organizations facing regulatory enforcement actions for failing to properly manage their third-party risks. A single adverse vendor event can seriously impair your operations, harm your customers, or cost your organization a lot of money in unplanned expenses, lost revenue, legal fees, and fines.

Poor quality products or services

Consider a vendor that provides a service to your organization, such as a marketing firm that emails your customers. If this vendor's risk is not actively managed, there's a possibility of poor-quality work that can lower your revenue, impact operations, and your bottom line.

Dissatisfied customers

Vendors that interact with your customers on your behalf could potentially act in a way that reflects poorly on your organization. Failing to manage your vendors' risk and performance can result in unhappy customers and even regulatory violations.

Increased inefficiencies

Third-party vendors can serve a variety of purposes, generally with an overall goal of creating more operational efficiencies. However, a vendor that isn't properly managed or monitored can create inefficiencies, disruptions, and added costs because of risk or performance issues that aren't noticed early enough to avoid or until it's too late to resolve.

Unintended cost

When contracts with third-party vendors are signed and filed away, your organization can incur unexpected costs. Unforeseen contract renewals, increased service costs, and unmanaged risks are all consequences of unmanaged third-party contracts. Your organization may be subject to unnecessary costs without TPRM.

04 | Use your data

Some stakeholders may respond better to your requests when they see the numbers that come directly from your organization. This provides real-world examples of the value of TPRM.

Data You Can Use:

The size of your vendor inventory

Reveals the extent of your organization's exposure to third-party risk. It can also highlight the cost and need for TPRM program buy-in from your stakeholders.

The number of critical and high-risk vendors

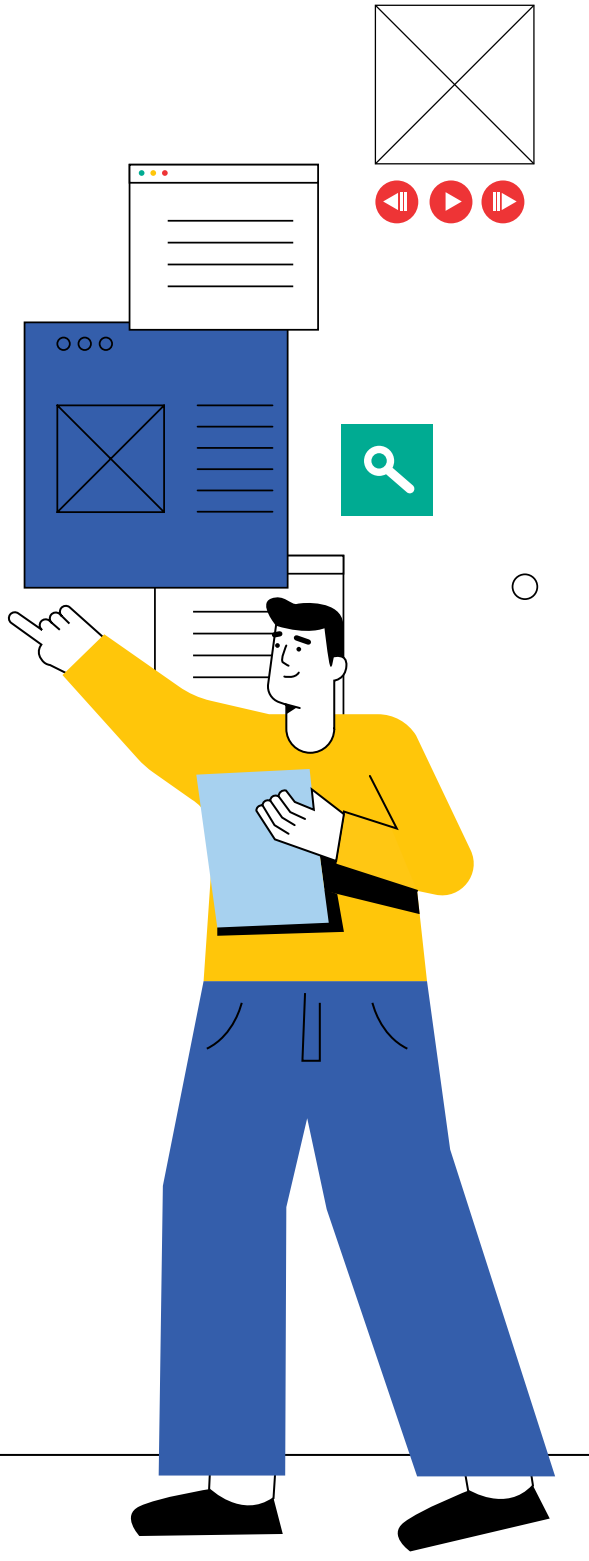
Supports your request for additional resources. These vendors require a higher level of due diligence and ongoing monitoring, which can be burdensome without enough resources.

The time spent for onboarding vendors

This may be excessive when there are more tasks than people to complete them. If the organization waits to onboard a vendor, certain opportunities may be missed, or problems may become worse.

Examples of data breaches, regulatory fines, and other real-world scenarios

Gives your stakeholders a grasp on the importance of TPRM. It's helpful to keep these relevant to your organization's industry.



PRO TIP:

How Many People Does It Take to Manage Vendors?

We recommend the following as a guideline for full-time employees (FTEs). This formula is appropriate if you're using an automated platform, with about 10-15% of your total vendor portfolio consisting of critical or high-risk vendors. There must be at least one senior member on this team to set the standards for TPRM. Take these things into consideration when you're calculating the number of FTEs.

- 1-3 FTEs for up to 300 vendors
- 3-5 FTEs for up to 500 vendors
- 1 additional FTE for every 200 vendors beyond that

Your organization might not be ready to add additional FTEs, but there are other options you can present to leadership. Outsourcing some processes might make more sense than adding staff.

venminder

05 | Present the options

Soliciting support from stakeholders will likely be easier if you've already done your research and documented a few options that will work well with your organization. Depending on your available resources and current needs, you might consider one of the following options:

Keeping your program in house

You'll need to first identify the people in your organization who are already involved in TPRM. Some may need to be brought in from other departments and educated on your strategic goals. This option may appear to be the most cost effective, but it's likely that you'll still need to invest in additional resources, like SMEs or other dedicated TPRM staff.

Implementing TPRM software

If your team is already familiar with the features they need, you might benefit from using a dedicated TPRM software. This can be a valuable tool for day-to-day management of a comprehensive program or providing just a few specific capabilities like vendor monitoring and contract management.

Outsourcing certain activities

Some organizations lack the in-house capacity for certain activities like collecting and reviewing vendor due diligence documents or creating program documents. Outsourcing these activities can ensure that your internal resources aren't spent on time-consuming tasks.

Creating a combination of solutions

After doing your research, you may discover that the best option is creating a custom combination of internal and external resources. Some of your program activities might be kept in-house, where your team can use TPRM software, and other processes can be outsourced so your organization doesn't have to invest in additional full-time employees.

TPRM may be an organizational mandate, but that doesn't automatically guarantee stakeholder buy-in. To foster understanding and stakeholder support, it's essential to communicate the many benefits of TPRM and how it protects the organization.

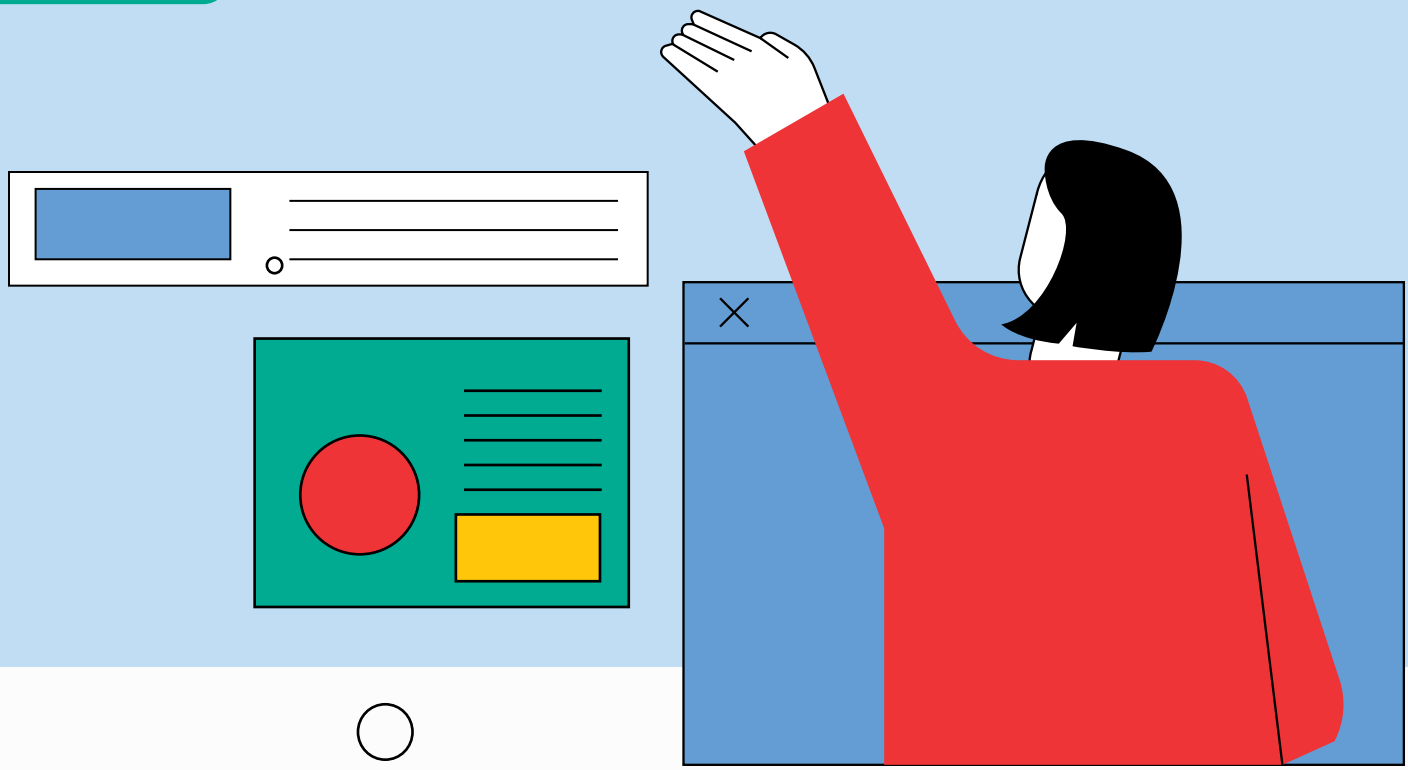
Furthermore, it's important to address any misconceptions or concerns about TPRM and present the options that will work best for your organization. After all, the best TPRM programs are those where all stakeholders are engaged and share a common vision of how to succeed.

Sources

- **SecurityScorecard.** (February 1, 2023). Close Encounters of the Third- (and Fourth-) Party Kind. SecurityScorecard. https://securityscorecard.com/blog/close-encounters-of-the-third-and-fourth-party-kind-blog/
- **IBM and Ponemon.** (2023). Cost of a Data Breach Report 2023. IBM. https://www.ibm.com/reports/data-breach
- **Reuters.** (February 28, 2022). Toyota suspends domestic factory operations after suspected cyber attack. Reuters. https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/
- **U.S. Securities and Exchange Commission.** (September 20, 2022). Morgan Stanley Smith Barney to Pay $35 Million for Extensive Failures to Safeguard Personal Information of Millions of Customers. U.S. Securities and Exchange Commission. https://www.sec.gov/news/press-release/2022-168

Download free 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.