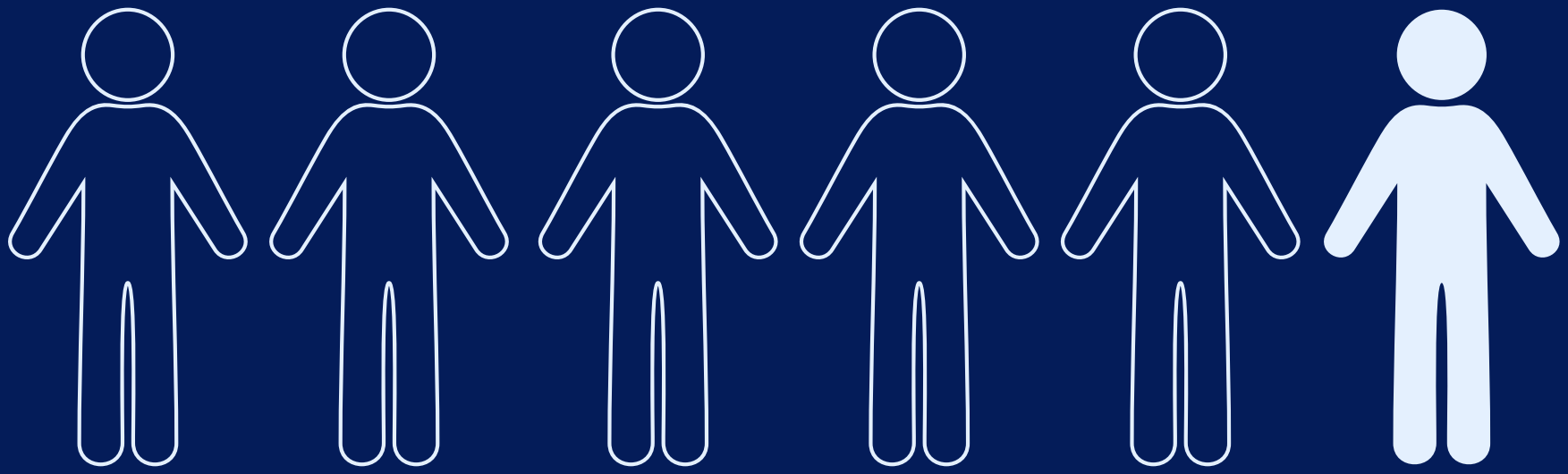
How Many People Should You Dedicate to Third-Party Risk Management?



venminder

How Many People Should You Dedicate to Third-Party Risk Management?

One of the most frequently asked questions surrounding third-party risk staffing is, “how many people should you dedicate to third-party risk management?”

Unfortunately, even regulatory guidance offers little assistance in this area, except for reiterating the importance of adequate staffing. The truth is that many organizations, regulated or not, continue to understaff their third-party risk management teams. And, the term “team” is often an overstatement as it is not uncommon to see TPRM responsibilities rest on the shoulders of a single individual. So, what is the right number? How many people does it take to ensure your third-party risk management program is operating effectively?

Let’s examine eight considerations, industry data, problems associated with understaffing, and a formula to help you decide how many staff members you need for third-party risk management.

Factors to Consider When Determining the Number of Third-Party Risk Management Staff

1

How complex is your organization?

Complex organizations usually require more people with specialized skills to address all elements of third-party risk management. As an organization grows, so does its vendor pool, which potentially means more critical and high-risk vendors. An organization with more critical or high-risk vendors must have enough people to perform more risk assessments, due diligence, and monitoring activities.

venminder

2 How much does your organization outsource?

Typically, the more an organization outsources products/services, the more people it needs to oversee those outsourcing efforts.

3 How centralized is your third-party risk management program?

The number of staff will vary depending on how centralized your third-party risk management program is.

- Does your organization depend on internal subject matter experts (SMEs) from across the organization to assist with vendor due diligence and risk reviews?
- Do vendor owners take responsibility for risk and performance management?
- How does your third-party risk management team interact with your enterprise risk team?

Suppose your program requires participation from many different departments. In that case, you may need to allocate more time and resources to coordinate your third-party risk management activities.

4 What activities must be performed by the third-party risk management team?

While certain activities, such as due diligence, could be delegated to other members of your organization, other tasks, including risk assessments, cannot. For smaller organizations, it might be possible to handle all your third-party risk management duties in a centralized environment. However, mid-sized to larger organizations cannot reasonably cover all third-party risk responsibilities with only a single full-time employee.

5 What are the regulatory requirements for your industry?

Industries such as financial services and healthcare are more strictly regulated than others. Your organization must ensure it can meet the requirements set by regulators for your industry. Consider your current practices, how stressful it has been to meet regulatory expectations, and whether you're prepared if regulatory expectations increase.

6 How many vendors do you have?

The level of effort and the specific actions required to manage vendor risk effectively can vary depending on the number of vendors and the risk level presented by each. However, the number of vendors is a significant factor when determining the number of staff.

When it comes down to it, every vendor engagement must undergo at least seven activities: planning, inherent risk assessment, due diligence, contracting, risk re-assessment, ongoing monitoring, and offboarding. To get the most basic idea of how many significant actions would be required, you could multiply the number of vendors you have by those seven activities.

If you have 500 vendors, that would be around 3,500 individual actions to be performed by the TPRM team – each requiring various levels of in-depth work. This estimate doesn't include the other TPRM activities like reporting, policy and program updates, issues tracking, and managing or training vendor owners.

venminder

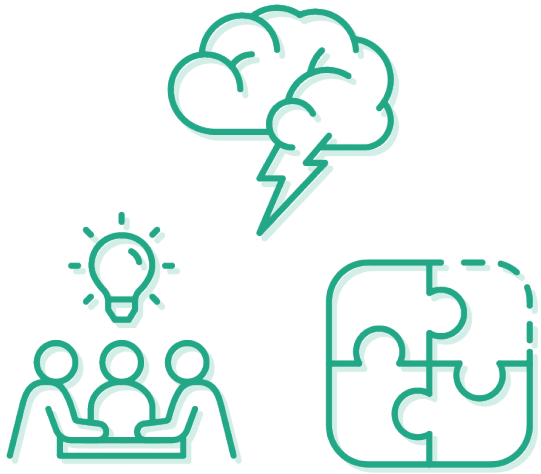
7 How effective are your third-party risk management tools and processes?

- Does the organization depend on manual third-party risk management processes?
- Or, does the organization use software and technology specifically designed for third-party risk management?

TPRM-specific software and tools can be a great way to create efficiencies within your program. Organizations can reduce their administrative workloads and the number of dedicated TPRM staff needed to get the job done by automating processes such as contract alerts, risk assessments, and vendor performance assessments. Conversely, manual processes are time-intensive, error-prone, and often require more dedicated staff.

8 How qualified is your third-party risk management team?

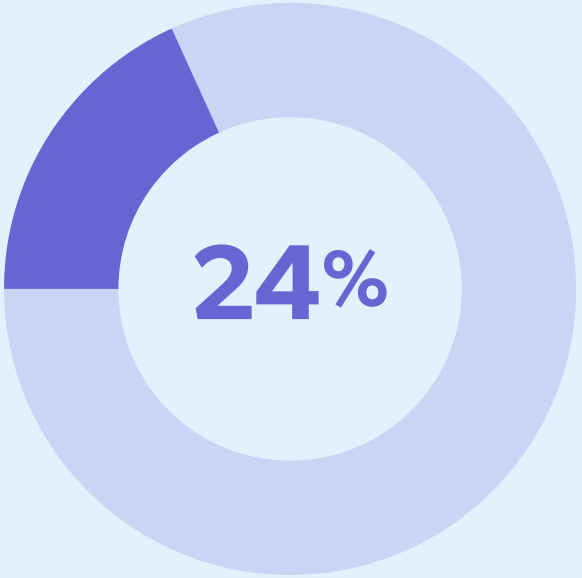
Although there is no set number of employees you should have on staff, it's important to ensure they have the skills and abilities to perform their tasks. Remember, it's about quality, not quantity. An oversaturation of inexperienced team members will be far less effective than a smaller team of knowledgeable experts.

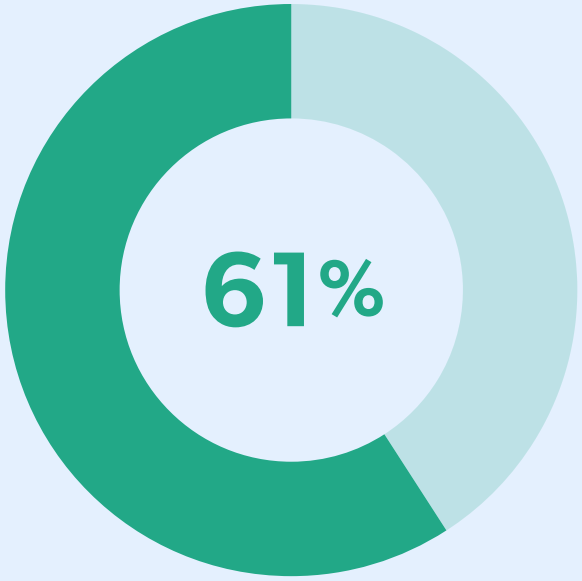


What the Industry Has to Say

According to our annual State of Third-Party Risk Management Industry Survey, 24% of organizations have 0 full-time third-party risk resources.

Likely, they either have a highly effective compliance officer who farms out the tasks, or it hasn't come up as an issue in a regulatory examination. Sometimes, third-party risk responsibilities are given to an already overburdened compliance officer, who is more concerned with consumer protection regulations until exam time or until a problem occurs.





Meanwhile, 61% of organizations have 1-5 full-time third-party risk resources.

That number may be too small for an organization to adequately complete the necessary work throughout the vendor risk management lifecycle. That lifecycle includes the following stages: onboarding, ongoing, and offboarding. Within each stage of the lifecycle, multiple activities and tasks are required, including documentation & reporting, independent review, and oversight.

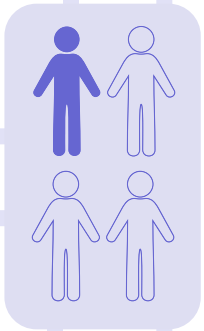
The Severe Problems with Understaffing for Third-Party Risk

Too Much to Manage

Failing to perform third-party risk management tasks effectively can significantly and negatively impact your organization. In cases where the workload has become too much for staff to keep up with, the impacts will snowball. For example, taking a shortcut during vendor due diligence could lead to missing a vulnerability in the vendor's security controls. That insufficient control could lead to a breach, resulting in reputational damage, fines from regulators, lowered customer trust, and revenue losses.

Relying on One Person for All of the Answers

If someone is out for an extended period, who can help in their absence? Giving the keys to the kingdom to only one person is a major risk. Not to mention that burnout from such situations is real and may cause your TPRM to seek employment elsewhere.



Lack of Subject Matter Expertise

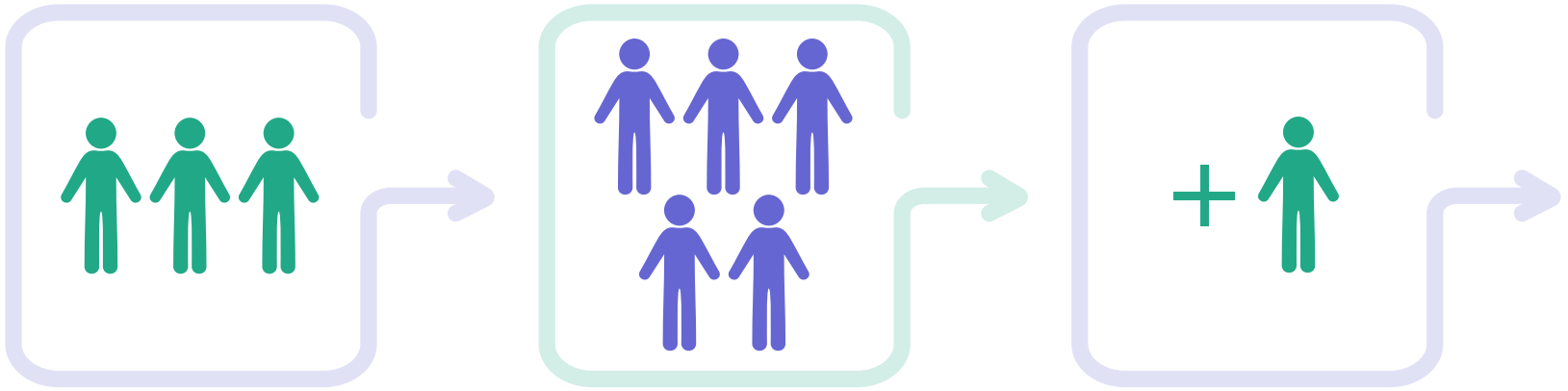
Third-party risk management can be complex. It requires skill and experience to perform effectively. It's possible to teach third-party risk management, but there is nothing to replace a seasoned professional with real-world experience. If an organization believes anyone can do it, they set themselves up for failure. Third-party risk management knowledge, experience, and sound judgment are key competencies to ensure success.

When it comes to performing vendor risk assessments as part of due diligence, subject matter expertise is also critical. There is a significant risk for organizations that rely on unqualified individuals to assess vendor controls. Qualified subject matter experts have significant experience in their respective risk domains and hold professional licenses and credentials.

The Third-Party Risk Management Staff Quantity Formula

Your formula will vary based on the type of organization and all the factors mentioned above.

This formula is appropriate when your organization uses third-party risk management software. It assumes that about **10-15% of your total vendor portfolio are critical or high-risk vendors** requiring annual risk assessments and a great deal of ongoing due diligence:



1-3 FTES
for up to 300 vendors

3-5 FTES
for up to 500 vendors

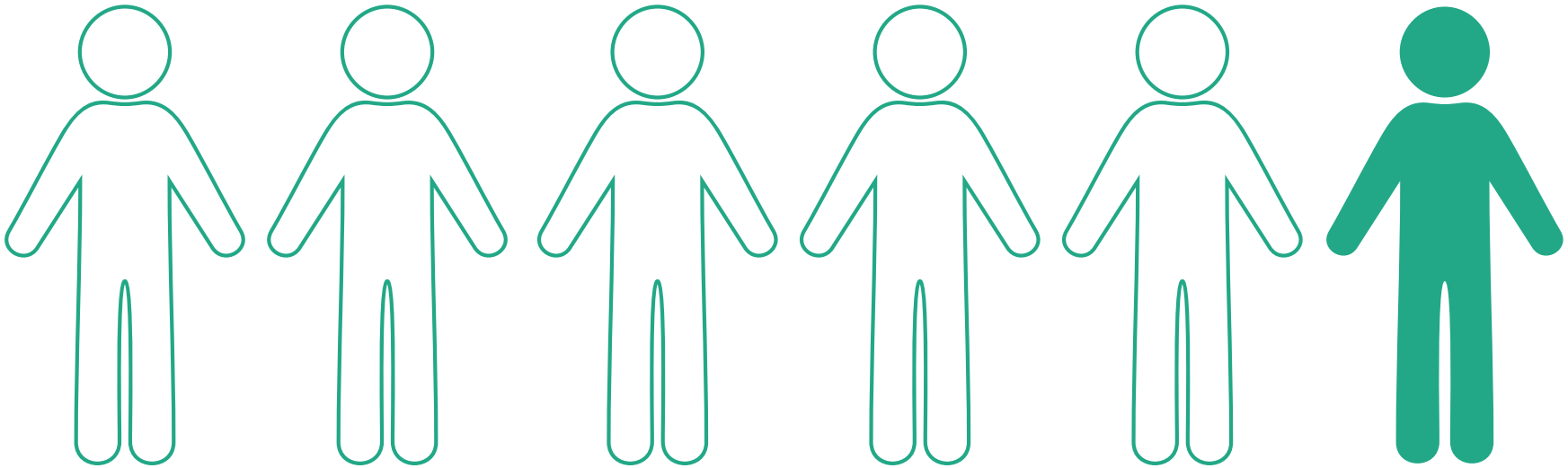
+1 FTES
for every 200 vendors beyond that

Pro tip: *If you can outsource portions of your third-party risk management program, you can save on both overhead and salary expenses while conducting third-party risk management at a lower expense than managing it in-house.*

venminder

Recognize the value of a well-run third-party risk management program and invest in the resources to do the job well.

It not only helps you meet regulatory expectations, but also creates better risk management, greater security, and greater value.



venminder

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

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.