venminder

State of Third-Party Risk Management

2024 Whitepaper

Table of Contents

Executive Summary

Venminder's State of Third-Party Risk Management 2024 survey provides insight into how organizations manage third-party risk today.

Results from the survey provide an in-depth look at current practices, challenges, compliance incentives, and third-party risk management benefits. For our eighth annual survey, Venminder surveyed individuals from a wide variety of organizations and industries, including financial services, fintech, retail, food services, insurance, healthcare, information technology, and more, in a nice balance of different sizes ranging from less than $1B assets or less than 100 employees to more than $10B assets or more than 5,000 employees.

Venminder promoted the survey publicly through email, social media, and the Third-Party ThinkTank online community from November 2023 through January 2024. Participants were allowed to provide anonymous, confidential answers to ensure the authenticity of their responses.

In 2023, there was no shortage of events and concerns to underscore the critical importance of effective third-party risk management programs. The sudden closure of three regional banks, the proliferation of artificial intelligence (AI) and its associated risks, and the release of the Interagency Guidance on Third-Party Relationships: Risk Management demonstrated that managing third-party risks has become much more complex than simply dealing with traditional "vendors." As a result, even the most experienced third-party risk management practitioners were prompted to re-assess the scope and effectiveness of their programs.

Expanding the scope of third-party risk management and its continuously emerging risks were only some of the many recent challenges. Managing well-known risks, such as cybersecurity, privacy, and operational resilience, has become more difficult due to the emergence of increasingly sophisticated cybercrimes, new data breach notification requirements, an upsurge in privacy regulations, both domestically and internationally, and a rise in global conflicts that has threatened supply chains worldwide. Given these developments, third-party risk management is more important than ever, and is becoming even more critical going forward for 2024.

While third-party risk management is a well-established practice, it's also continuously evolving. Organizations of all sizes and industries must continually adapt and change to effectively identify, assess, manage, and monitor third-party risks.

By analyzing the third-party risk management landscape and practices captured in our survey, organizations can see where they stand compared to their peers and consider that information as they prepare and implement changes this year and beyond.

We would like to express our gratitude to our 2024 survey respondents, who generously shared their knowledge and experiences, providing valuable insights into real-world third-party risk management challenges and opportunities.

Survey Highlights

Venminder's State of Third-Party Risk Management 2024 survey offers insights from peers on current third-party risk management processes, best practices, challenges, and the emerging risk landscape.

Here are just a few highlights:

1 Third-party risk management **programs run lean and may be getting leaner.**

2 Most organizations believe there is **ROI in third-party risk management activities.**

3 **Cybersecurity remains a top priority** and concern.

4 **Artificial intelligence is an emerging top risk** for third-party risk management programs.

5 Organizations are **feeling the pressure from regulators** to improve third-party risk management.

6 **Using risk intelligence tools to monitor** third, fourth, and nth parties is growing in popularity.

Survey Results

Size and Makeup of Vendor Landscape

Size and Makeup of Vendor Landscape

It's crucial to remember that third-party risk management programs can differ significantly – each organization has its unique outsourcing approaches. Some organizations outsource most of their work, while others prefer to manage more activities in-house. Therefore, the number of third parties being managed doesn't necessarily correspond to the size of an organization.

Regardless of size, organizations must clearly understand who they're doing business with and the products and services those third parties provide. However, knowing how many third parties are under management is only part of the equation; knowing the risk and criticality of those third parties will help organizations better estimate the effort and resources required to manage those relationships effectively.

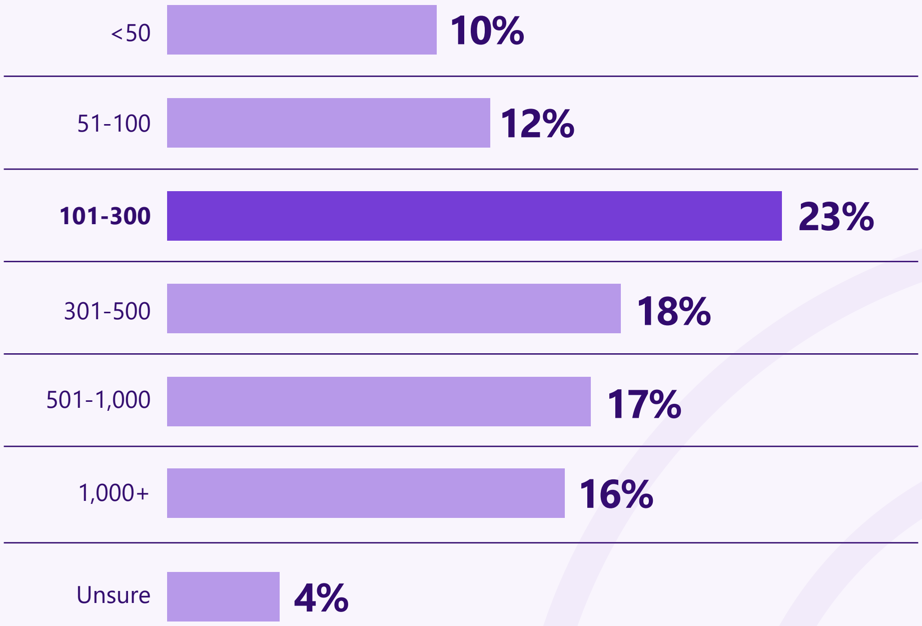
For this reason, comprehensive and current third-party inventories are a must. Our survey indicates that organizations are paying attention, and only 4% of respondents indicated they were unsure of how many third-party vendors they had, down from 11% in the previous year.

Program Size

The number of organizations with small (under 100 vendors), midsize (101-500 vendors), and large (501-1,000 vendors) programs remained stable, while very large (1,000+ vendors) programs increased by 5% compared to the previous year. This increase could possibly be attributed to new regulatory requirements.

For instance, the Interagency Guidance on Third-Party Relationships: Risk Management was finalized in July 2023 and it clarified third-party relationships as any business arrangement by contract or otherwise, excluding those with customers, which dramatically increased the scope of third-party risk management for many organizations. The purpose of this clarification was to ensure third-party relationships that were not previously part of typical third-party risk management programs, such as fintech, revenue sharing, banking relationships, and even subsidiaries, were visible and subject to third-party risk management requirements. This includes risk identification, assessment, management, and monitoring.

How many total vendors are included in your third-party risk management program?



Critical Vendors

Third-party inventories are most useful when they identify the relationships providing critical products or services to your organization or customers. As a best practice, critical shouldn't be used as risk rating, but rather as an indicator of which relationships are most important to maintain your operations, support your customers, and avoid regulatory scrutiny. There should be clear, formalized criteria to determine if a product or service (and therefore the third-party relationship) is in fact critical.

Organizations can use the following three questions to aide in that determination:

- Would a sudden loss of this vendor cause a disruption to your organization?
- Would that disruption impact your customers?
- If the time for the vendor to recover operations exceeded 24 hours, would it negatively impact your organization?

If your answer to any of these questions is "yes," you're likely dealing with a critical third party.

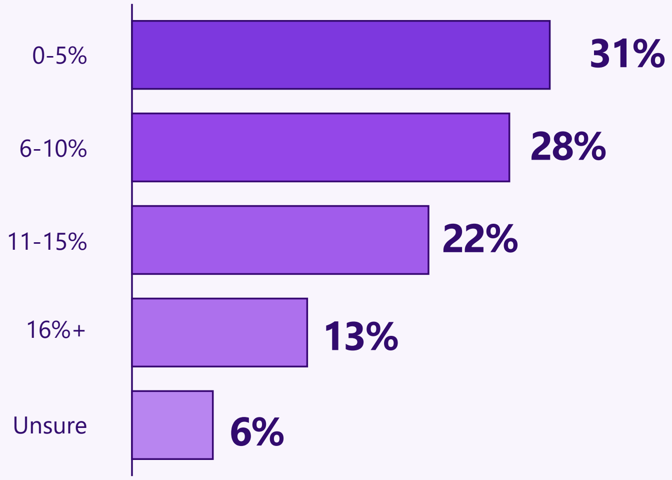
It's important to understand that not all products or services are essential to your business operations or can impact your customers. Therefore, you need to identify which third parties are truly critical to your operations and manage the risks associated with them with the appropriate intensity and at the right intervals.

Generally, a good rule to follow is that no more than 15% of your total vendor inventory should be considered critical.

Most of our respondents are well within the 15% guideline, although 13% did cite a critical vendor inventory of more than sixteen percent (16%). Only 6% are still unsure, which is an improvement on last year's eight percent (8%).

What percent of your vendors would you classify as business critical?

(The sudden loss of those vendors would disrupt your business, impact your customers, or would require more than 24 hours to recover normal operations.)



If your percentage is higher than 15%, it may be time to re-examine those relationships and ensure the criteria is appropriately applied. While it's possible for organizations to have higher percentages of critical vendors within their inventory, labeling too many vendors as critical without meeting the criteria, or incorrectly categorizing them, can raise concerns for auditors and examiners. It can also cast doubts on third-party risk management processes and overburden your resources.

Reporting Structures, Operating Models, and Organizational Support

Reporting Structures, Operating Models, and Organizational Support

Developing a robust and efficient third-party risk management framework plays a critical role in the success of any organization. To achieve the best results, it's important to establish a reporting structure that aligns with third-party risk management's purpose, maximizing its effectiveness. Moreover, adopting a third-party risk management operating model that maximizes available risk management resources, skills, and experience helps achieve the desired risk management outcomes.

Along with reporting structures and operating models, it's essential to have dedicated third-party risk management resources and tools that promote a proactive and resilient third-party risk management framework.

Third-Party Risk Management Reporting Structures

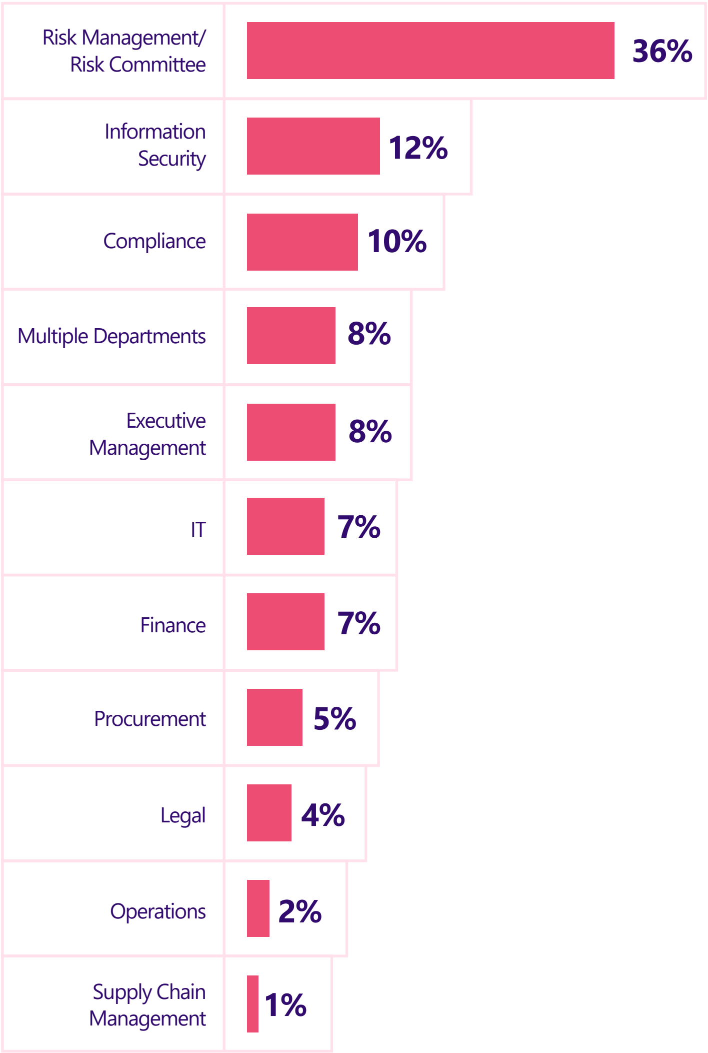
The success of an organization's third-party risk management program can be significantly influenced by where it sits within the organization. Third-party risk management programs are most effective when they're integrated into reporting structures that support their function as a true risk management discipline. The program is meant to address and manage a distinct set of risks associated with external relationships.

Alignment with established risk management structures and departments, such as Risk and Compliance, can improve third-party risk management's visibility, elevate program credibility, and increase internal third-party risk management compliance.

Nearly half (46%) of our respondents report their third-party risk management programs to Risk Management or Compliance. While it's widely acknowledged that aligning third-party risk management with a risk-focused department or function is a best practice, there are other organizational alignments that could also be effective.

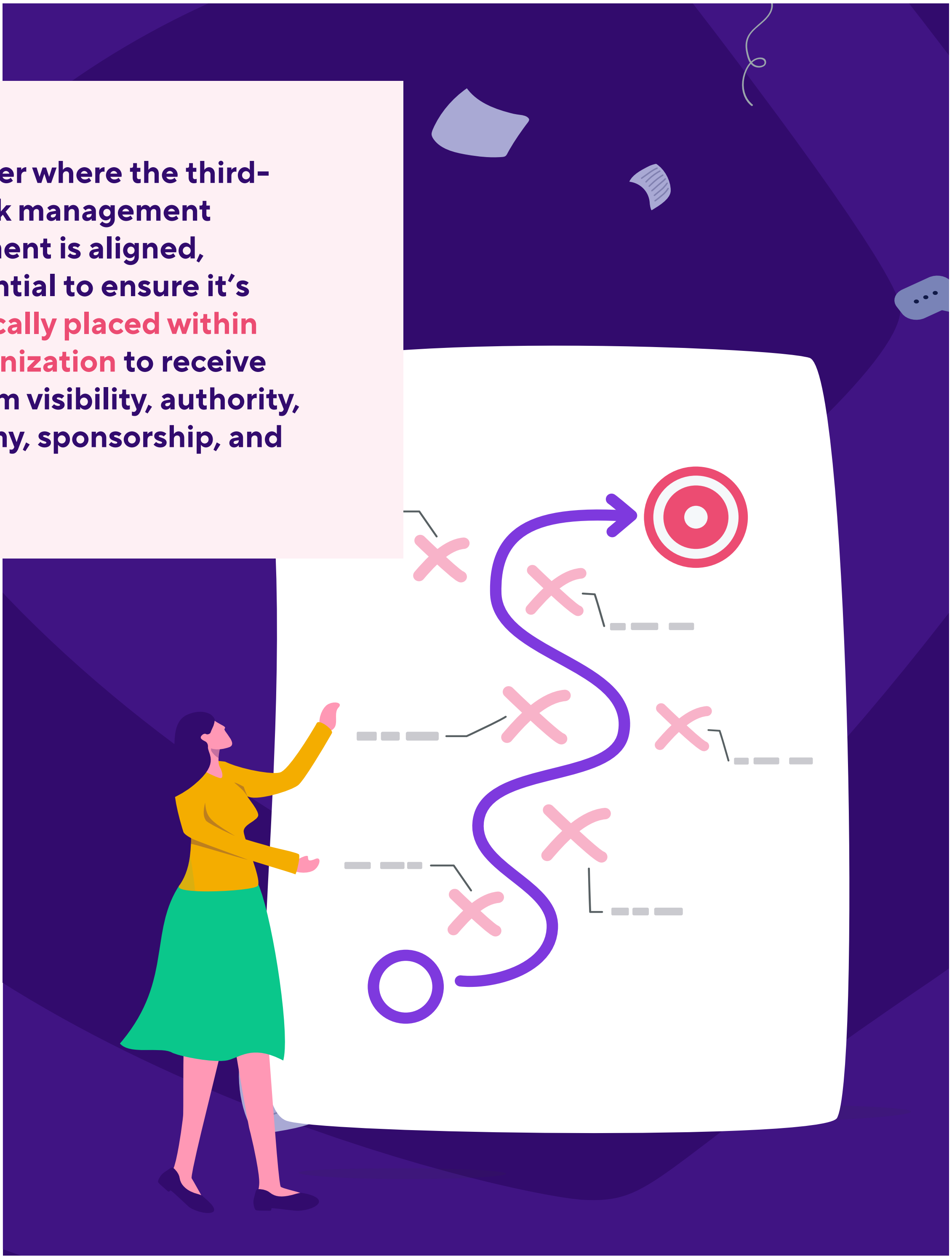
Every organization has its own unique structure, and many have successfully implemented third-party risk management programs in different environments. Nineteen percent (19%) of third-party risk management teams report to IT and Information Security departments, as there is often a close relationship between information security and third-party risk management, making it a highly effective reporting structure for many organizations.

Which department does third-party risk management report to?



Other organizations have found success aligning third-party risk management within their Finance, Sourcing, Procurement, or even Legal departments. This highlights the flexibility of third-party risk management programs and the diverse range of options available to organizations, enabling them to choose the best fit for their specific needs.

No matter where the third-party risk management department is aligned, it's essential to ensure it's strategically placed within the organization to receive maximum visibility, authority, autonomy, sponsorship, and support.



Operating Models

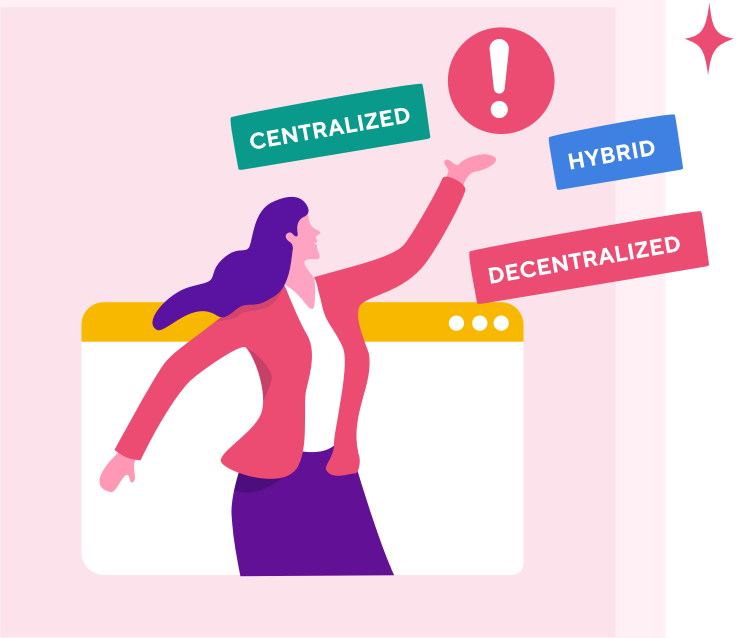
Reporting structures determine where third-party risk management reports within the organization, but the third-party risk management operating model determines how tasks are accomplished and by whom.

There are three common operating models for third-party risk management:

Centralized – All third-party risk management functions are conducted by the same dedicated team.

Hybrid – Functions are shared between a dedicated third-party risk management team and vendor owners/the lines of business.

Decentralized – Functions are managed across teams without any dedicated third-party risk management team.



It's not uncommon for organizations to change their third-party risk management operating models at different stages of program maturity. For example, an organization just starting their third-party risk management journey may operate in a decentralized model until a dedicated team can be established.

This year's survey results indicated that **centralized models are still the most popular**, at 52%, although this number is down from 60% last year.

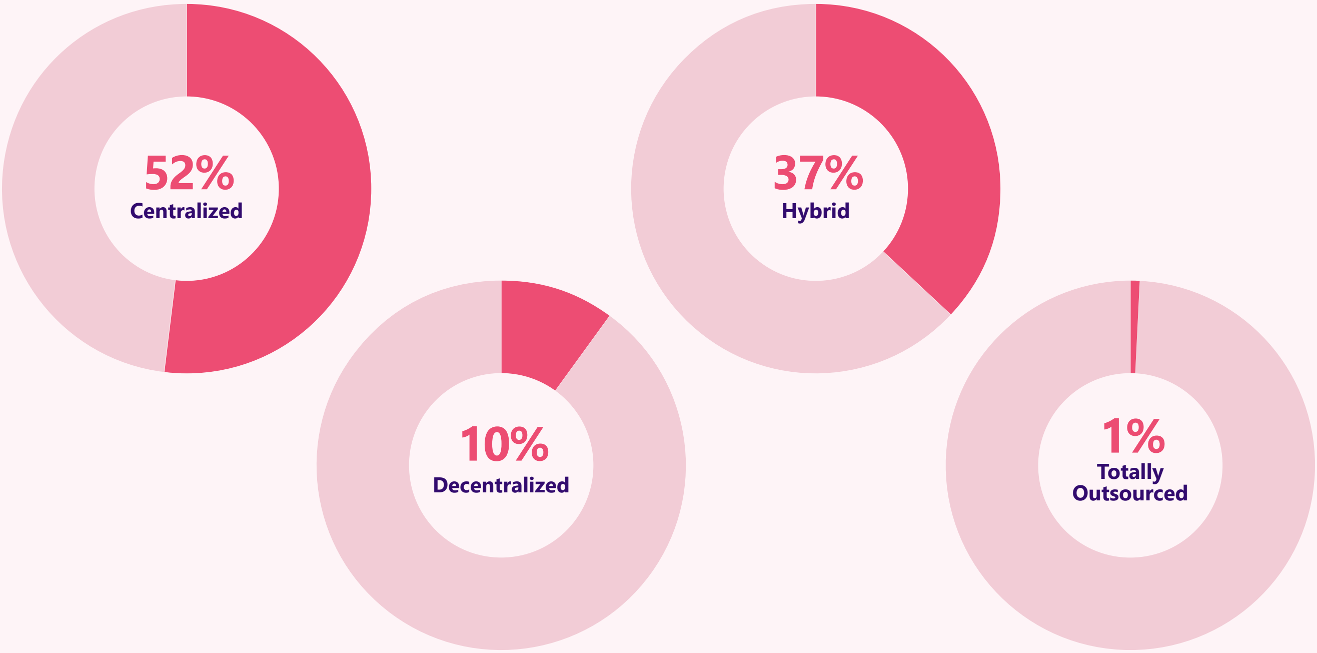
When it comes to managing third-party risk, a centralized model can be practical and effective. Responsibility and accountability are located within the same team, which can ensure more consistent delivery of key third-party risk management tasks and reduce dependencies on the business unit – business units/lines refer to the different teams or divisions responsible for products, services, or functions within an organization (i.e., marketing, product, research and development, finance, and operations). However, there may be some downsides to this model. The vendor owner, who is usually in the business line, may not be fully engaged in managing the risk, resulting in less proactive risk identification and delayed remediation efforts. Additionally, vendors may be confused about who they ultimately report to and what should be prioritized.

Hybrid models are still a popular option, but their popularity seems to vary from year to year. Last year, only 29% of organizations reported using them, but this year, 37% of organizations now use hybrid models – so more organizations are switching over to this model.

The advantage of hybrid models is that a dedicated third-party risk management team maintains the program's structure and flow, ensuring everyone stays on task and accountable. However, individual vendor owners are still responsible for managing vendor-level risks, and subject matter experts across the organization perform vendor risk reviews. For hybrid models to be effective, everyone in the organization should be aware of risks and manage them appropriately according to their roles.

Ten percent (10%) of the survey participants reported using a decentralized approach to manage their operations. **Decentralized models are often adopted by organizations when first starting their third-party risk management efforts.** However, they tend to shift to other models as they refine their operations. This shift is typically due to various challenges commonly experienced in a decentralized model, such as inconsistent management of third-party risks, incomplete documentation and reporting, and difficulties gathering required information due to the lack of a specific team responsible for the program. Additionally, third-party risk management activities may not be prioritized against other business goals and may remain unaddressed.

What operating model do you use for your third-party risk management program?



Only 1% of organizations totally outsource their third-party risk management function. Outsourcing specific third-party risk management activities, such as vendor due diligence document collection or SME reviews, can be a good option when the organization needs more resources or expertise.

However, it’s important to note that outsourcing the entire third-party risk management function isn’t recommended. Maintaining an internal purview and accountability for third-party risk management within the organization is crucial.

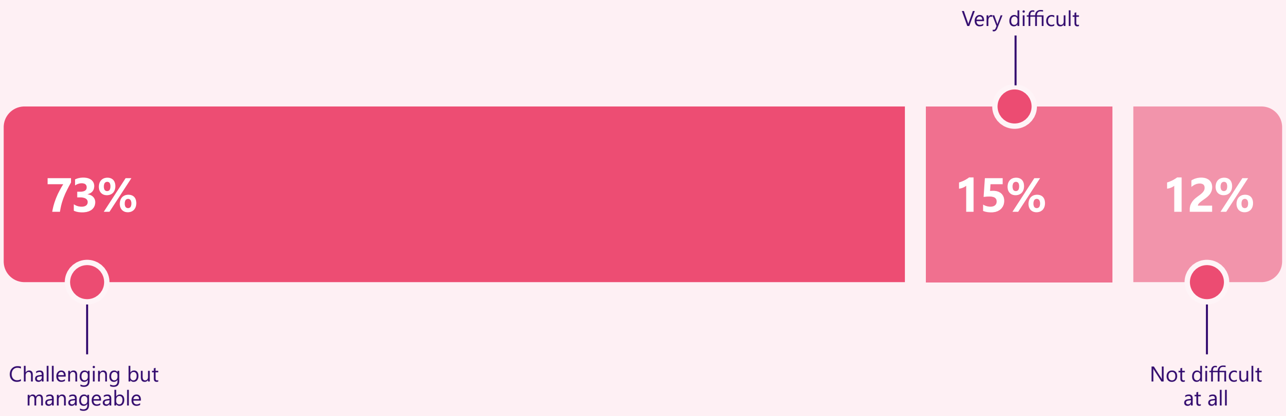
This approach also ensures a better understanding of third-party risks and their impacts on the organization.

Organizational Support

Although third-party risk management programs may have effective operating models and ideal alignment within the organization, they can still be less effective due to poor support from business lines and vendor owners. This lack of support may manifest in several ways. For instance, business lines may not prioritize third-party risk management activities, or may consider them secondary to their primary business goals. In other cases, business lines or vendor owners may resist assigned roles and responsibilities within the third-party risk management process. A more common challenge faced by third-party risk management teams is the difficulty of chasing late or missing deliverables from vendor owners.

Consistent with previous surveys, third-party risk management teams still encounter difficulties in obtaining the required support from the business units or vendor owners. According to survey respondents, 73% of the teams found it challenging, yet manageable, while 15% find it very difficult.

How difficult is it to secure vendor owner/business unit support for your third-party risk management program?



A significant lack of support can have a real impact on the effectiveness of the third-party risk management teams, and it can put the businesses in jeopardy. However, for the 12% of the teams that found it easy, the secret may be having a strong tone-from-the-top and effective management from the middle.

Third-party risk management support from business units and vendor owners is heavily influenced by the tone-from-the-top. Senior leadership plays a crucial role in the effectiveness of the third-party risk management program, and their actions and words have a direct impact on the organization. When there's a lack of funding or insufficient resources, it sends a message that third-party risk management is not a priority.

Furthermore, if business lines aren't following requirements and leadership seems unconcerned, it can lead to third-party risk management being perceived as just another "check-the-box" activity.

It's not just about the tone-from-the-top; it's also about management from the middle. Every level of management must work together to translate the top-down approach into daily attitudes and behaviors that reinforce the importance of third-party risk management and ensure its effective execution. This requires incentivizing managers to ensure third-party risk management is a priority for their teams.

One way to achieve this is by including third-party risk management key performance indicators (KPIs) in personnel performance reviews and holding vendor owners accountable for delivering third-party risk management on time and with high quality. By doing so, business line management can ensure their teams are fully committed to third-party risk management, and that the organization is well-positioned to manage third-party risks effectively.

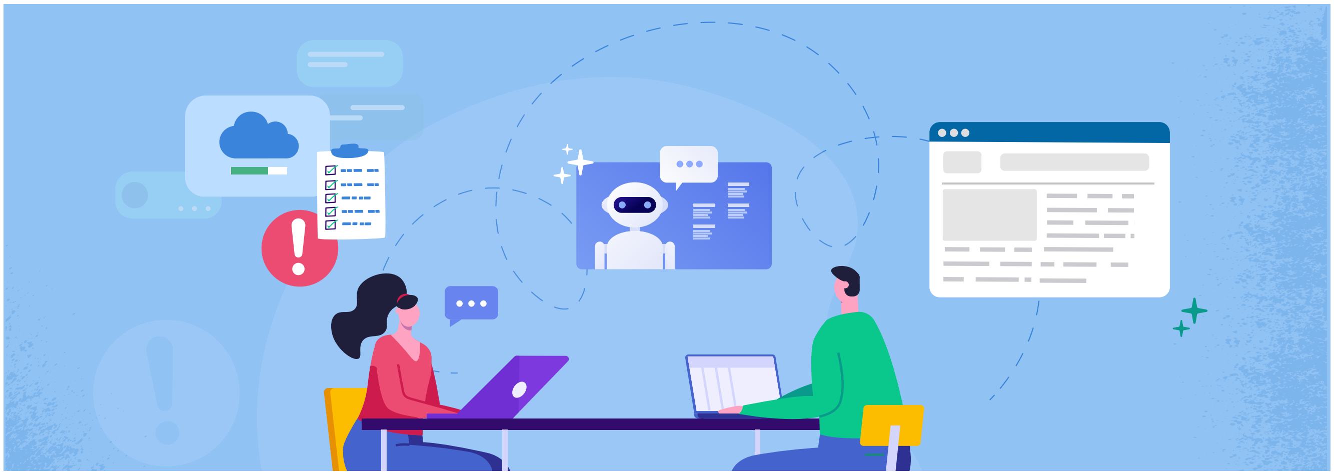
Third-Party Risk Management Resources, Technology, and Tools

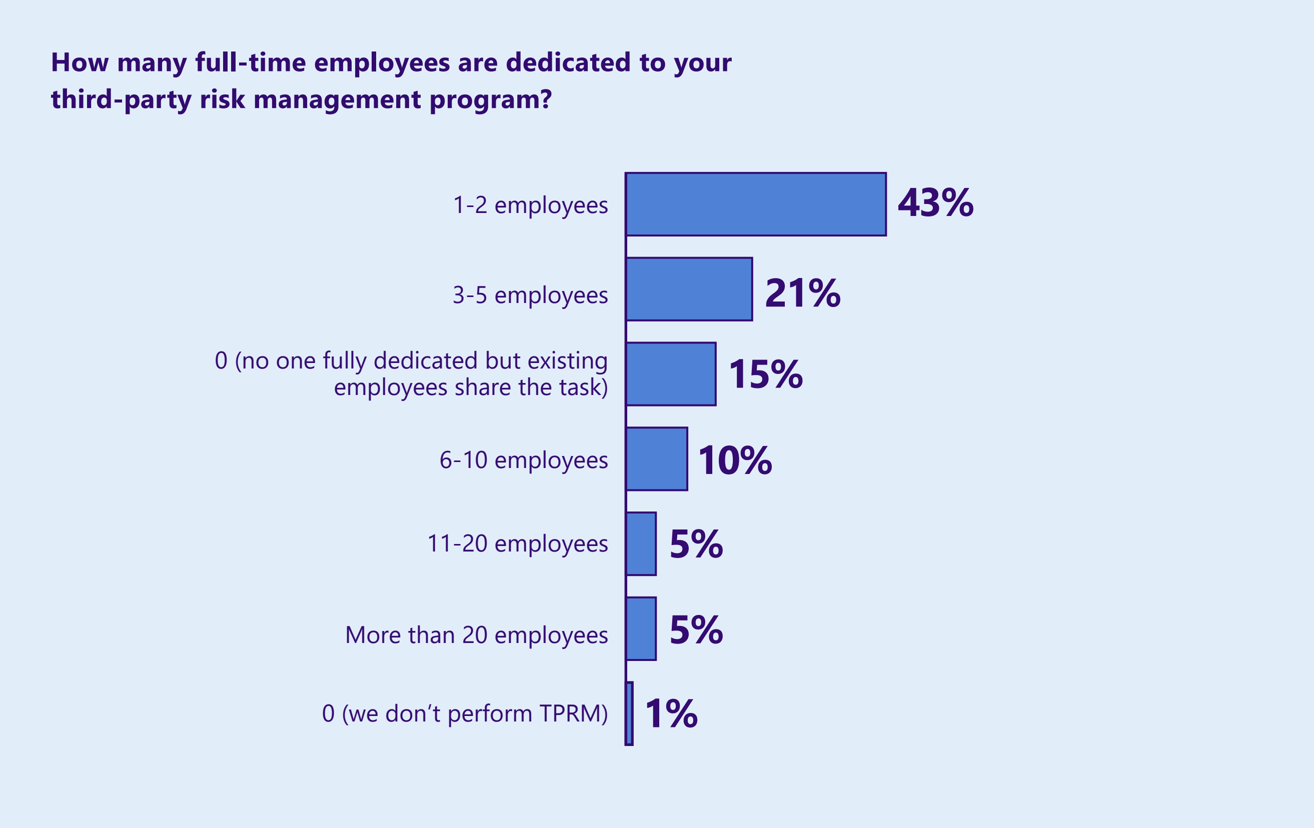
Third-Party Risk Management Resources, Technology, and Tools

Third-party risk management is a complex practice that requires expertise and knowledge, which are honed with practical experience. However, considering the number of vendors to manage, even in smaller organizations, it becomes extremely challenging for individuals to oversee third-party risk management program activities while performing other functions. This is where dedicated staff come in. Having an adequately staffed team with the right skills will ensure proper focus on the oversight and execution of the many tasks involved in third-party risk management.

There's no set number of personnel required for third-party risk management, but every organization should have adequate and skilled staff to carry out the program efficiently and effectively based on the organizations' unique needs. Third-party risk management programs can benefit from utilizing technology to achieve more efficient and effective results, too.

By implementing standardization and automation, and improving data collection and reporting, third-party risk management teams can increase their capacity even with limited resources.





Dedicated Staff

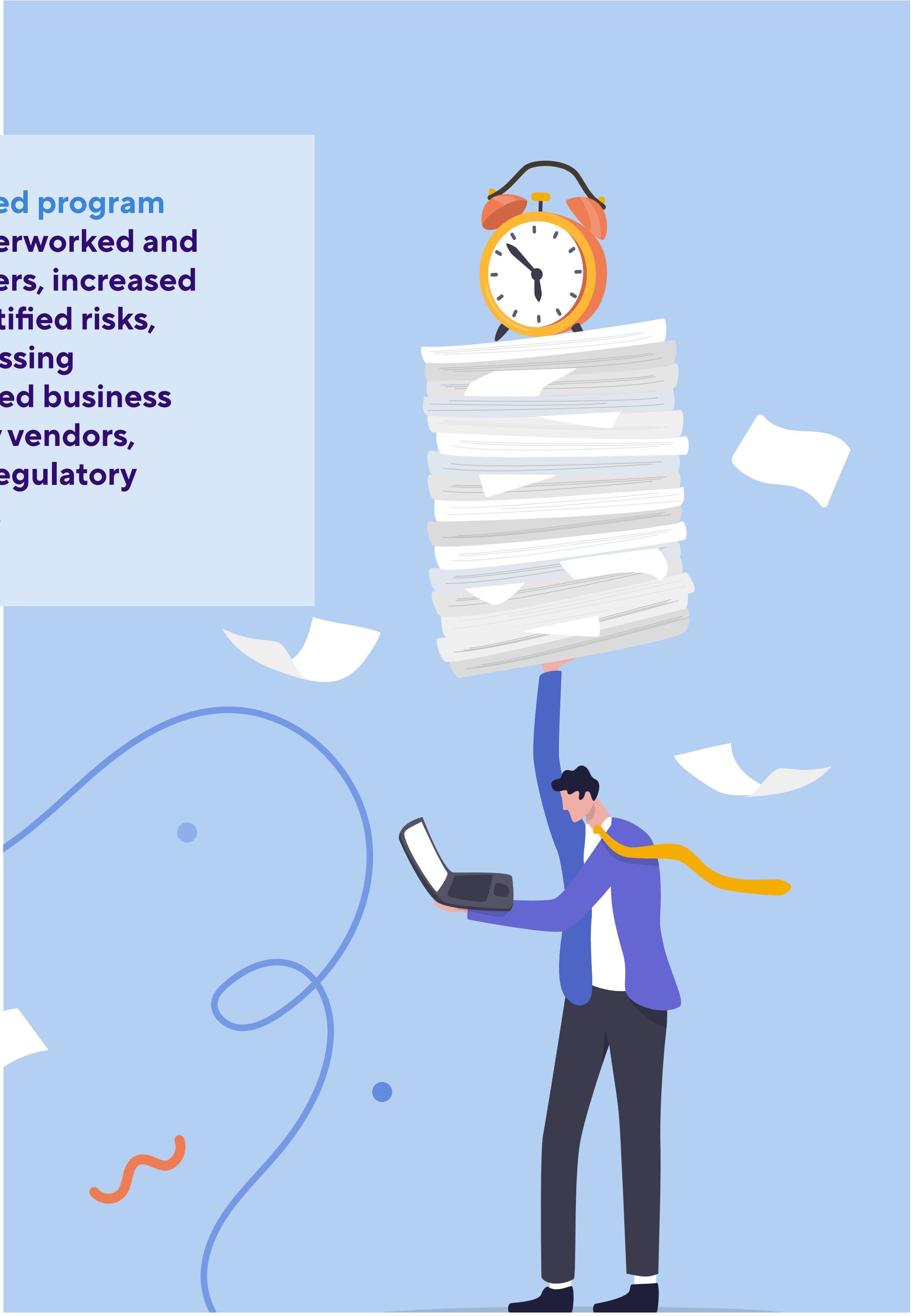
Third-party risk management programs require sufficient staffing with qualified personnel for success. The number of dedicated employees needed for a program depends on various factors, such as how many vendors are being managed, operating model, and the level of organizational support for the program. However, even the most experienced third-party risk management practitioner can only do so much in a day.

According to our survey, 43% of respondents have no more than two dedicated third-party risk management employees and 21% reported having 3-5 employees. Organizations with 5 or fewer dedicated third-party risk management staff account for 64% of participating organizations. This is consistent with results from previous surveys.

It's worth noting that while third-party risk management teams have typically been small, they might be shrinking, particularly in larger organizations. While the number of programs with 6-10 employees has slightly increased from 6% in the previous year to 10% in 2023, this doesn't necessarily indicate that third-party risk management teams are growing overall. It's possible that larger teams – those with more than eleven employees – may be undergoing staff reduction or rightsizing. As an example, only 5% of responding organizations this year said they had more than 20 third-party risk management employees, compared to 8% in last year's survey.

Still, 15% of organizations don't have any dedicated third-party risk management employees. Even in a decentralized model, it's advisable to have at least one dedicated employee who can take ownership and responsibility for the third-party risk management framework, policy, and program.

An understaffed program can lead to overworked and stressed workers, increased errors, unidentified risks, delayed processing times, frustrated business lines, unhappy vendors, and possible regulatory repercussions.



Third-Party Risk Management Tools

Third-party risk management requires the careful coordination and management of various processes, inputs, and outputs. These activities are often time-critical and require meticulous record keeping to ensure compliance with regulations and industry standards. To manage and document these complex activities, organizations use a wide range of methods and tools.

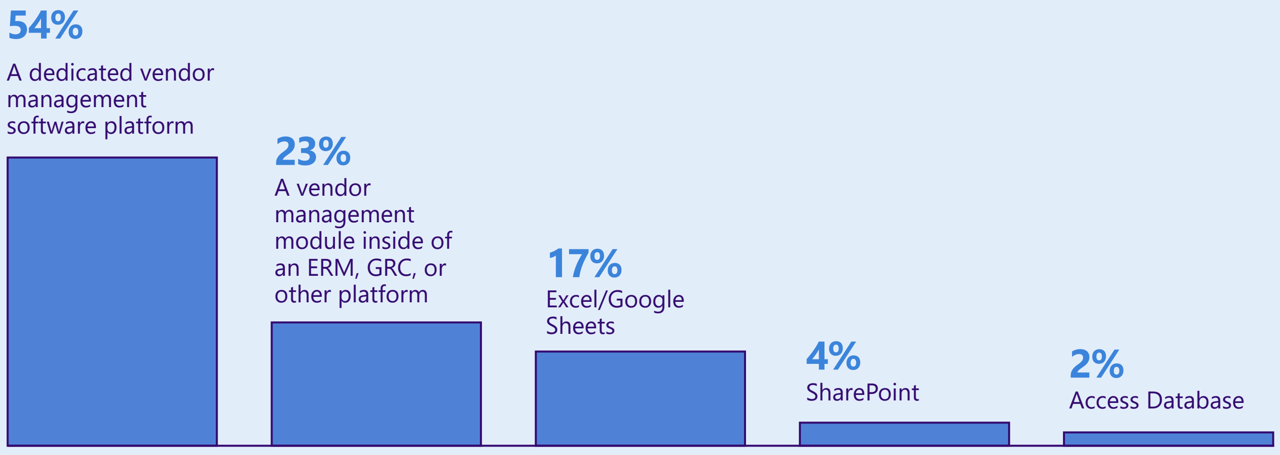
According to our survey, 77% of respondents now rely on software with vendor management features and functionality to streamline the management of vendor risk.

Fifty-four percent (54%) of those respondents use a dedicated third-party risk management software that is specifically designed to address the various processes and complexities involved in third-party risk management.

Most dedicated platforms are easily scalable as your third-party risk management program matures. They provide basic and advanced functionality and workflows needed to help manage the required activities and processes in the third-party risk management lifecycle.

In addition, they offer internal and external communication and collaboration functions and serve as an all-in-one document repository. These software tools replace outdated manual methods and tools, which are often slow to execute and prone to errors.

What is your primary tool for managing vendor risk?



Twenty-three percent (23%) of respondents are leveraging third-party risk management modules within another system, such as enterprise risk management (ERM) or governance, risk, and compliance (GRC) tools. While these tools are a step up from manual processes and generic tools, ERM or GRC applications typically focus on managing an organization's overall risk and are often limited in features and sufficient functionality to efficiently manage the intricate, specialized requirements and workflows associated with third-party risk management.

The remaining 23% of organizations use manual processes, relying on generic tools like Excel, SharePoint, and Access. This could be due to the fact that many organizations are just beginning to develop and implement third-party risk management practices at their organization and are using the tools readily available to them that don't require any additional investment. Organizations with less mature third-party risk management programs tend to adopt simpler practices in the beginning. However, as these organizations' third-party risk management programs become more established, they gradually adopt more advanced practices that typically require more sophisticated tools to manage.

In the end, the most important thing is ensuring third parties and their risks are effectively identified, assessed, managed, and monitored. This will look different for every organization, and it's important to remember that no tool alone will manage your third-party risk management.

Best Practices in Third-Party Risk Management

Best Practices in Third-Party Risk Management

Vendor Criticality

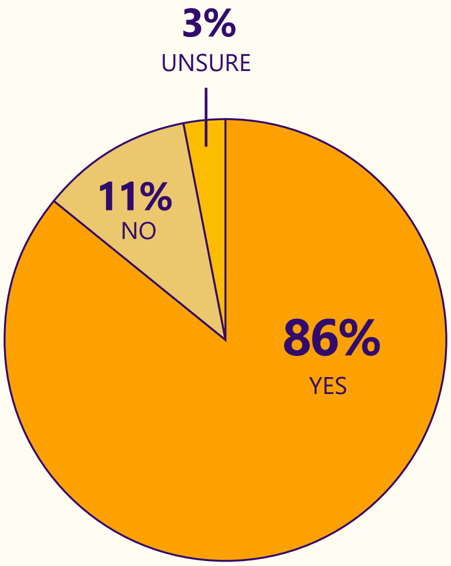
Critical vendors are those that are essential to an organization's daily operations. To minimize the disruption caused by critical vendor failure, organizations must conduct thorough due diligence, draft well-crafted contracts, and monitor both their risk and performance.

Critical vendors are often included in an organization's business resiliency planning, and auditors and regulators typically prioritize an organization's critical vendor relationships for review.

For these reasons, **organizations need to have a defined set of criteria to identify their critical vendors.** It's encouraging to see that 86% of organizations have established this practice, which is the highest percentage ever reported in our annual survey.

However, it's concerning that 11% of respondents still lack a process for identifying their critical vendors. Although this percentage is low, organizations need to understand the significance of this process as an essential part of managing third-party risk and complying with many regulations.

Do you have a formal process in place to determine criticality for all new vendors pre-contract?



Inherent Risk Assessments

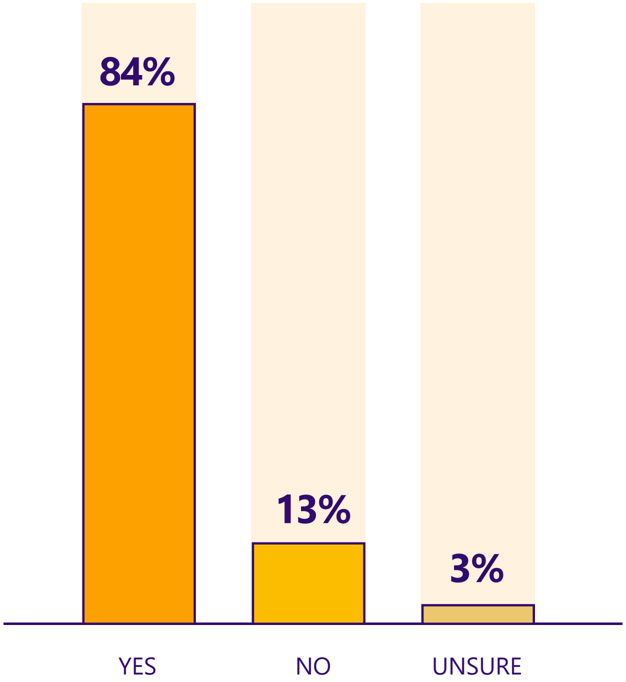
Our recent survey focused on organizations' practices of vendor risk assessment and rating. We aimed to learn how many organizations follow the best practice and regulatory requirement of assessing the inherent risks of all vendor relationships before signing a contract. We're happy to report that an overwhelming majority (84%) of respondents adhere to this principle, which is the highest ever reported in our survey. This is a positive trend as it ensures third-party risk management activities are based on inherent risk, which is an essential factor in the risk management process.

Sixteen percent (16%) of organizations either did not have or were unsure about their inherent risk assessment practices.

An organization that lacks formal inherent risk assessment processes not only risks scrutiny from auditors and examiners, but will struggle to identify and effectively manage third-party risks.

It's anticipated that with the continued advancement of newer programs, there will be a gradual decrease in the number of programs lacking inherent risk assessment processes.

Do you have formal risk assessment processes in place to determine inherent risk for all new vendors pre-contract?



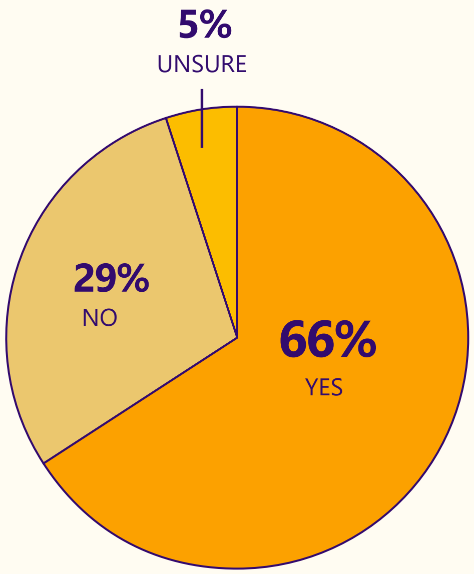
Residual Risk Assessments

Residual risk is the amount of risk that remains after the application of risk management practices and controls have been considered. It's important to evaluate the residual risk to manage risk effectively and ensure vendor engagements align with your organization's risk tolerance. By considering the vendor's controls and your organization's risk appetite, it's possible to determine whether the remaining risk level is acceptable. Assessing the residual risk of every vendor engagement can ensure appropriate risk mitigation and monitoring are in place and provide a comprehensive view of the risk across your vendor portfolio.

As part of a positive trend, 66% of the respondents do have formal processes in place to assess residual risk. However, a significant number (34%) either don't have an established process or are uncertain about residual risk in the context of third-party risk management. This may be attributed to the ongoing development of the concept of residual risk in many industries.

The residual risk rating should never be used as a replacement for or supersede the inherent risk rating. Residual risk ratings reflect the level of confidence in a vendor's controls, while inherent risk ratings establish the requirements for managing the vendor, including the extent and type of due diligence necessary, the frequency of re-assessment for risk, the structure of the contract, and the prerequisites for risk and performance monitoring and management.

Do you have formal risk assessment processes in place to determine residual risk for all new vendors pre-contract?



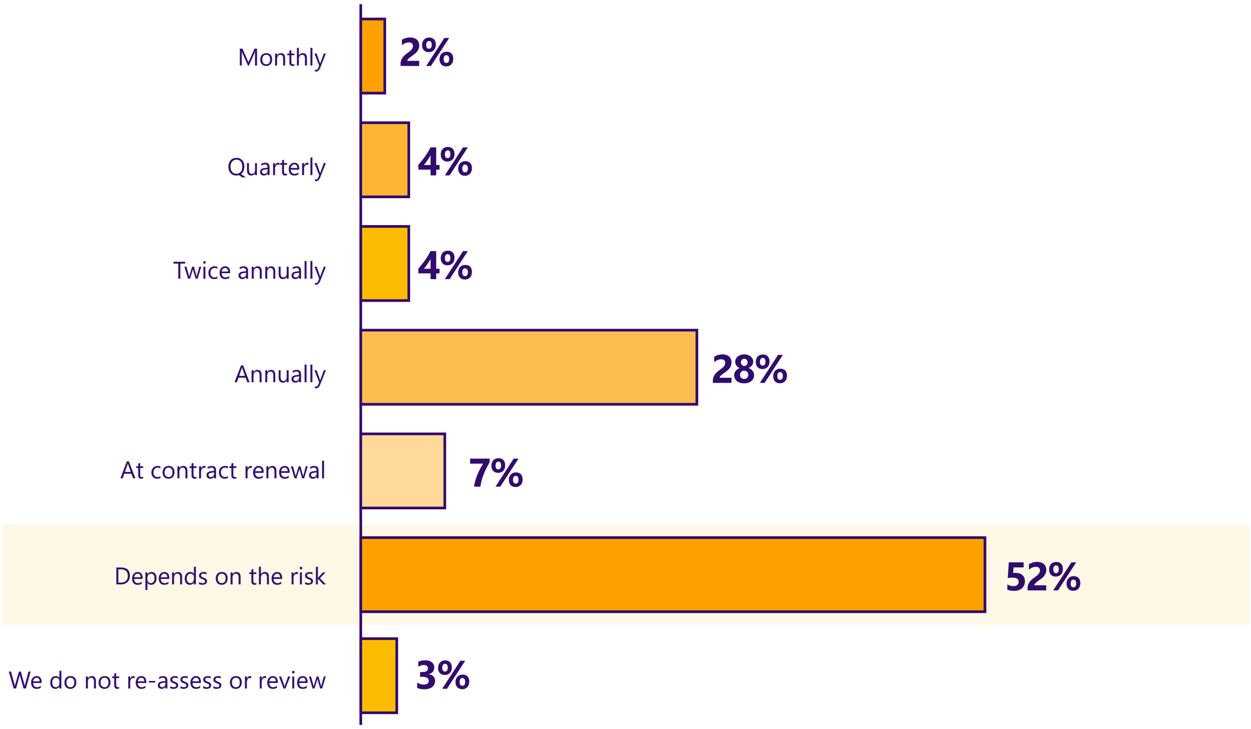
Risk Re-Assessment and Due Diligence

Performing regular risk re-assessments and collecting updated due diligence documents are crucial tasks for the ongoing identification, assessment, and management of risks, especially for high-risk or critical vendors. As risk profiles can quickly change, delaying re-assessments or only conducting them during contract renewal can increase the chances of overlooking new or emerging risks before it's too late, resulting in operational issues, negative financial impacts, or even regulatory repercussions.

Risk can always change, so avoid relying on one-time risk assessment exercises. However, the frequency of periodic risk re-assessments or reviews should always match the risk and criticality of the vendor relationships.

Using a risk-based cadence to determine the proper intervals for risk re-assessments and due diligence document collection is a rapidly maturing practice, and 52% of respondents aligned the frequency of re-assessment with the risk presented by the engagement.

How often are you reviewing and re-assessing vendor risk profiles and documentation?



At least 28% of respondents reported re-assessing or reviewing their vendors annually, which is the minimum recommended interval for critical and high-risk vendors.

Others reported different frequencies, but without added context, it's not clear what is driving those intervals or if they are risk-based. Of those surveyed, 7% only perform risk re-assessments before renewing a contract, while 3% don't perform any re-assessments at all.

It's imperative that organizations **adopt a re-assessment process that is robust and risk-based** to effectively manage third-party risks. Vendors' risk profiles can change over time, rendering once-effective controls weak and ineffective. This, coupled with external factors such as regulatory changes or industry shifts, can create significant gaps in a vendor's risk management practices or controls.

To stay ahead of these challenges, it's crucial to adopt a risk-based approach to determine the intervals for re-assessing risks, updating due diligence documentation, and reviewing them.

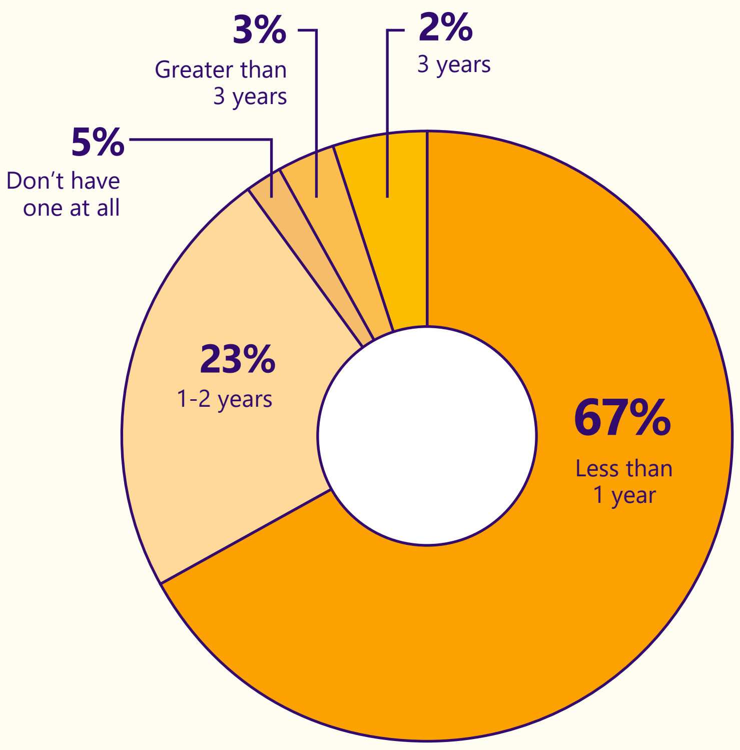
Current Policy

Establishing a third-party risk management policy is a fundamental first step for any effective program. The policy formally communicates all rules and requirements for third-party risk management within your organization. A strong third-party risk management program is dependent on a policy that is current and follows regulatory guidance and best practices.

At a minimum, the policy should be reviewed (and updated as necessary) at least annually. This is a best practice and a regulatory requirement. The release of new or updated regulatory guidance, or significant changes within your third-party risk management program, can be drivers for urgent off-cycle policy reviews and updates.

The recommended annual policy review is practiced by 67% of survey respondents. Twenty-three (23%) percent conduct policy reviews and updates every one to two years, which is an increase from the previous year's sixteen percent (16%). Another 5% report intervals of three years or more. A small percentage of programs (5%) are without any policy, which is a decrease from the previous year's eight percent (8%).

When is the last time you updated your third-party risk management policy document?



Updated Inherent Risk Assessments

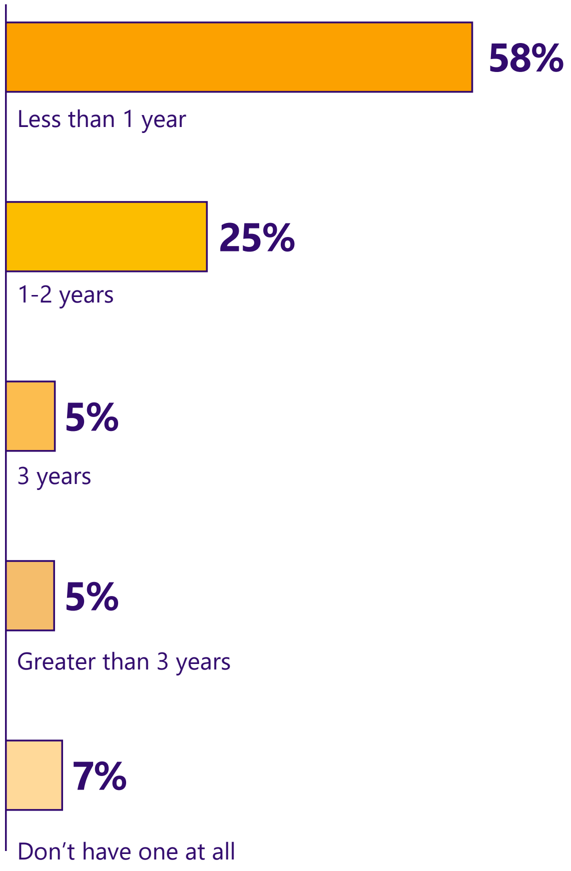
As the business landscape evolves, the risks associated with our third-party relationships also advance. Before the COVID-19 outbreak, it was impossible to imagine the global pandemic in our modern world. Four years later, we're still dealing with its impact. AI has become an essential aspect of our daily lives, whereas just a few years ago it was considered to be more or less science fiction. Cyberattacks have become more advanced and targeted, taking advantage of the massive amounts of digital data we generate, and ransomware attacks and data breaches have become commonplace.

When it comes to risk, it's always evolving and changing. The risk concerns we had a few years ago may not be as relevant today as they once were or may even become exacerbated with the progression of time.

Our recent survey results revealed that 58% of the respondents updated their inherent risk assessments within the last year, and 25% updated theirs within the last one to two years. This shows that a significant portion of participants recognize the importance of keeping their assessments up to date. However, 10% of respondents reviewed every three years or longer, and 7% didn't conduct any inherent risk assessments at all.

The foundation for successful risk management lies in effective risk identification. As a third-party risk management practitioner, it's important to remain knowledgeable about emerging risks and ensure your third-party risk management processes can effectively identify them. As such, it's recommended that you **keep your inherent risk assessments current by reviewing and updating them at least once a year.**

How recently have you updated your inherent vendor risk assessment?



Updated Vendor Due Diligence Questionnaires and Documentation Requirements

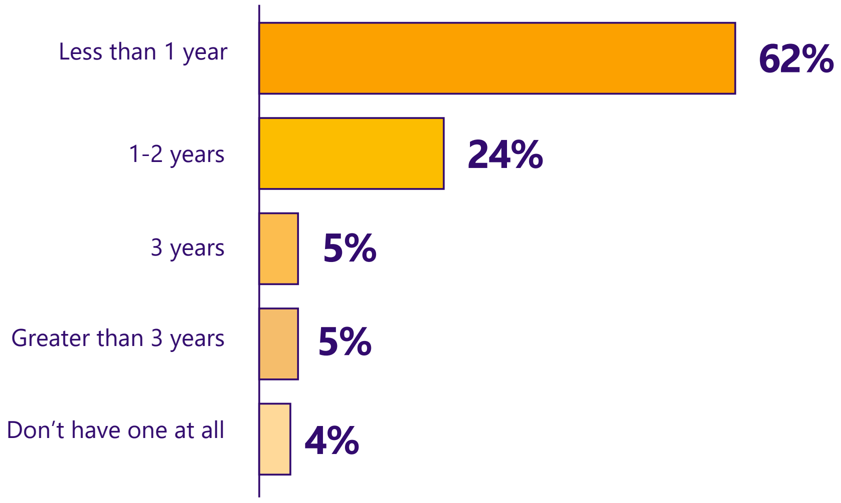
Just like your inherent risk assessment, you need to **review and update your vendor due diligence questionnaires and documentation requirements annually** to make sure they're reflective of current risk concerns, are comprehensive, and are up to date. Subject matter experts (SMEs) should be part of the team reviewing and updating the vendor risk questionnaires to ensure their accuracy and comprehensiveness.

By updating questionnaires and documentation standards, organizations can better determine if the vendor's risk management practices and controls are sufficient to address known risks. Keeping questionnaires current also sends a message to vendors that the organization takes risk management seriously and is dedicated to maintaining high-compliance standards.

It's great to see that the majority of survey respondents follow the best practice of updating their due diligence questionnaires and documentation requirements on a regular basis. Sixty-two percent (62%) of the participants reported updates within the last year, with an additional 24% having updated within 1-2 years. This is a slight increase from the previous year.

It's crucial for programs to understand the importance of having current and essential data gathering tools. Due diligence questionnaires and documentation requirements should be updated at least once a year, or whenever there are new material risks or regulatory changes.

How recently have you updated your vendor risk questionnaire and due diligence document requirements?



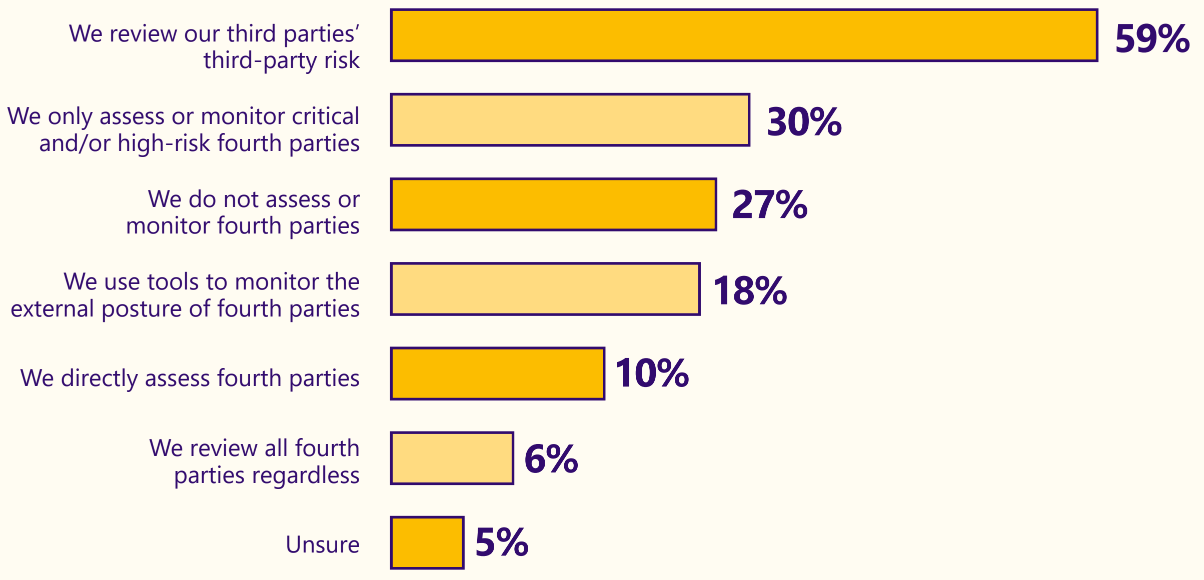
Managing Fourth-Party Risk

Managing risks associated with third-party vendors has become more challenging in today's business environment because the risk landscape has expanded to include fourth and nth parties. Fourth parties are a company or entity that has a direct contract with your vendor, but not with your organization. Nth parties extend beyond third and fourth parties. It can be difficult to effectively manage the risks of extended vendors. Therefore, we were interested in learning about how organizations are addressing this issue.

As per best practice, 59% of organizations are currently examining and assessing their vendors' third-party risk management practices. It's essential to understand how your vendors manage third-party risks and ensure they can provide proof of their essential third-party risk management processes, such as identifying critical relationships, evaluating inherent risks, conducting due diligence, and monitoring. **When it comes to managing third-party risks, your vendors should meet the same standards as your organization or have higher standards.** Verifying these practices during initial due diligence, and again through regular risk re-assessments and reviews, is a best practice.

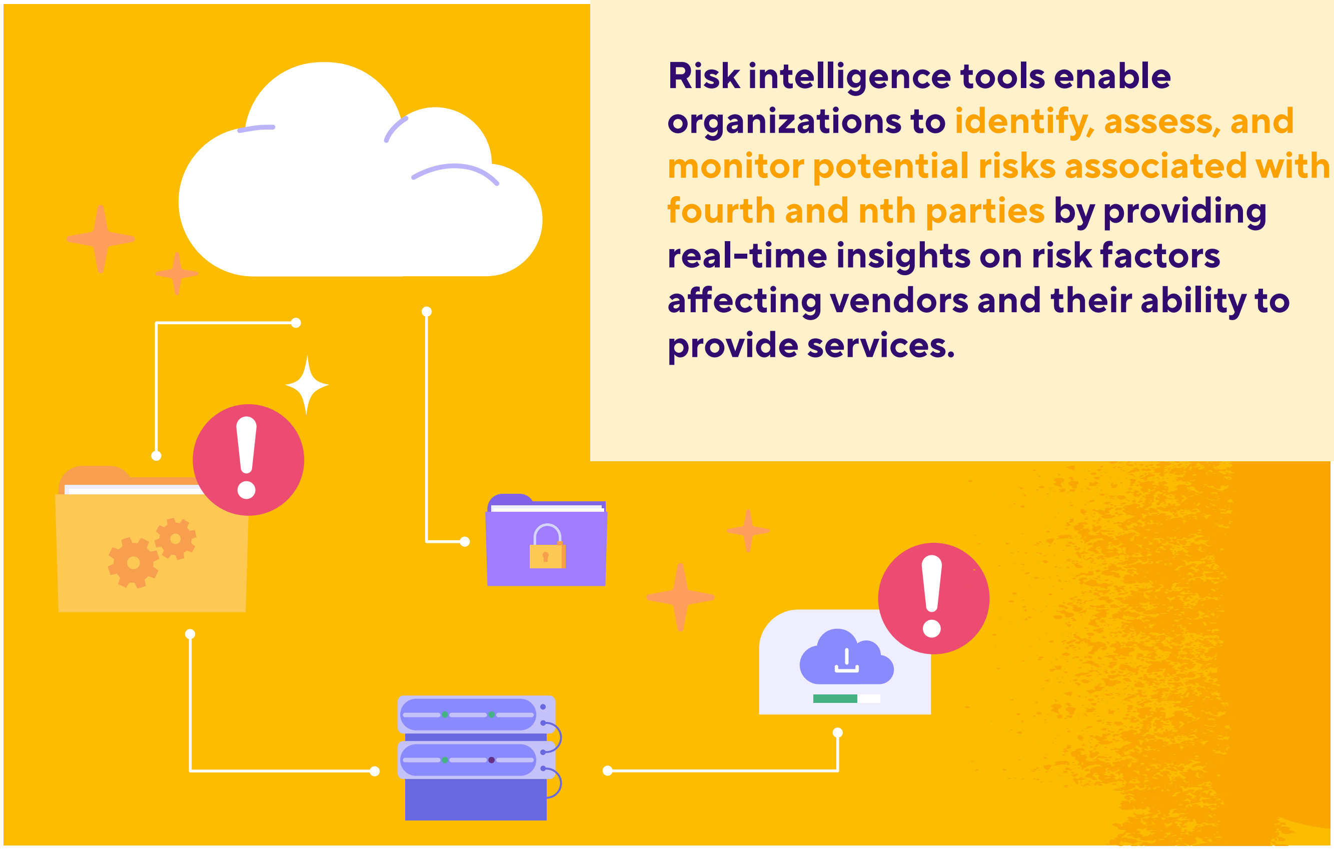
Some vendors might not have adequate or any third-party risk management practices. Hence, a different approach is required to manage risks associated with fourth and nth parties. Only 10% of organizations conduct direct assessments of fourth parties. While this approach is possible, it isn't often practical, as it can be hard to obtain information and documentation related to due diligence from a vendor with whom your organization doesn't have a direct contract.

How does your organization review fourth-party vendors/subcontractors?
*Respondents were asked to select all that applied.



Another 30% of organizations are either directly assessing or monitoring only critical and high-risk fourth parties. Six percent (6%) of respondents reported reviewing all fourth-party relationships. However, it's unknown what these processes involve and how effective they are.

Per the survey, 18% of organizations are using risk intelligence tools to monitor risks associated with fourth parties. **This approach is growing in popularity as it's highly efficient and effective.** It doesn't require any legal agreement between your organization and the fourth party, like a contract or nondisclosure agreement (NDA). Various risk intelligence providers offer one-time risk reports or continuous monitoring and alerts for any organization you choose, be it your direct third party, fourth party, or nth party.



Risk intelligence tools enable organizations to identify, assess, and monitor potential risks associated with fourth and nth parties by providing real-time insights on risk factors affecting vendors and their ability to provide services.

With risk alerts, organizations are notified of any changes or emerging risks such as changes in financial status, legal issues, or security breaches. Risk intelligence tools are an excellent complement to any organization's third-party risk assessment and monitoring processes.

Third-Party Risk Management Growth and Pressures

Third-Party Risk Management Growth and Pressures

Maturity of Third-Party Risk Management Programs

Organizations are making remarkable strides in their third-party risk management programs. A third (33%) of the organizations surveyed have already established and implemented third-party risk management programs, while another 38% are committed to improving their existing programs. This gradual yet steady improvement of third-party risk management programs is a clear indication of the critical role they play in an organization's risk management strategy.

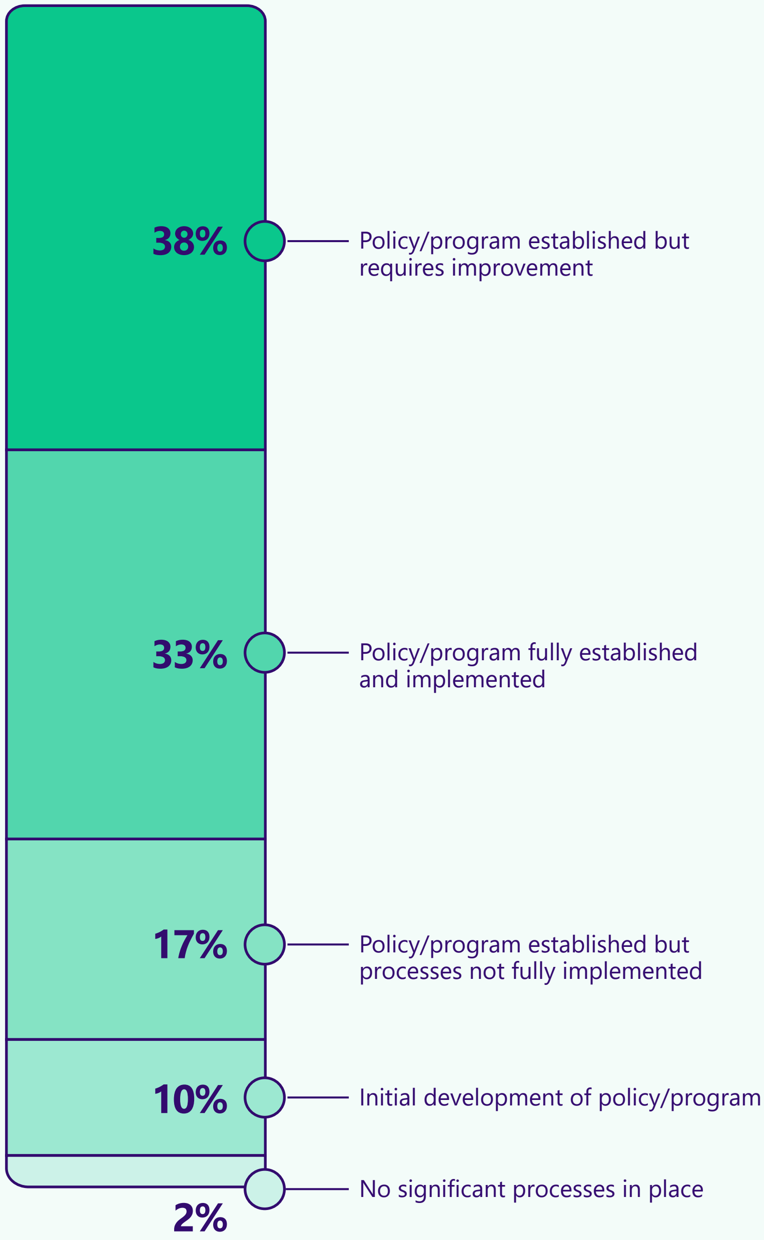
The survey further reveals that 17% of the participants surveyed are still in the initial stages of establishing programs and implementing processes, while another 10% are just getting started.

Third-party risk management is now fully being realized as an essential practice, and the majority of organizations are taking measures to establish and fully integrate third-party risk management processes.

Only 2% of the participants reported having no processes in place, an improvement on last year's five percent (5%). It's clear that third-party risk management is here to stay.

These results should encourage organizations that have not yet implemented third-party risk management programs to recognize the importance of it as a practice and take steps to establish and implement third-party risk management processes.

What stage of development is your third-party risk management program at?



Third-Party Risk Management Program Metrics

Many organizations are interested in measuring the health and success of their third-party risk management program and working on methods to show how third-party risk management adds value to their business. Establishing third-party risk management program metrics is the best way to evaluate and measure health, stability, and effectiveness in a comprehensive manner. They can be helpful when determining what improvements must be made and how to prioritize them.

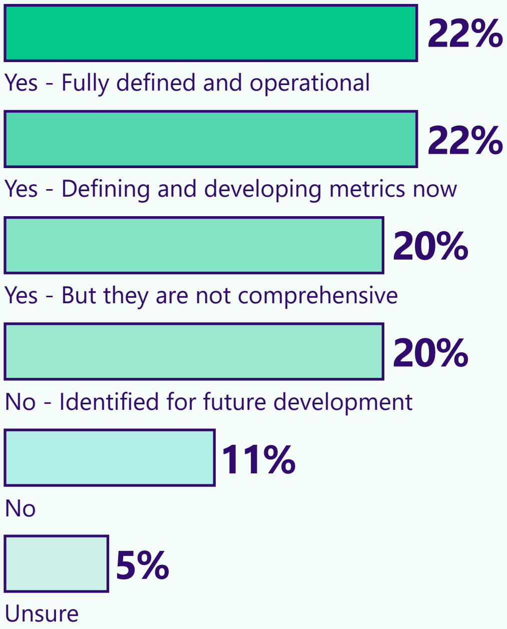
Moreover, third-party risk management program metrics can be used to predict where the program may be exposed to additional risks through a lack of resources, ineffective processes, or low internal compliance.

Third-party risk management program metrics are an area of increasing focus. Overall, 84% of respondents recognized the need for them and are at varying stages of development and implementation.

Programs with fully defined and operational metrics account for 22% of the organizations surveyed, while another 20% had some metrics but they were not yet comprehensive.

Collectively, another 42% were either developing metrics now or planning to in the future. Those that had no metrics or were unsure only accounted for 16% of the survey, which was down from 20% in the previous year.

Does your organization have defined metrics to measure the health, stability, and effectiveness of the third-party risk management program?



Audits and Regulatory Examinations

Audits and regulatory examinations should be expected in third-party risk management, so it's important for organizations to anticipate and prepare for them. According to our survey, only 10% of respondents did not have an audit or regulatory exam in the past year. For those who did, 28% received feedback that improvements were needed, while another 17% received no specific comments.

A considerable number of participants (37%) had gone through an audit or exam with no findings. This number shouldn't be attributed to simple luck, but is more likely the result of hard work, commitment to continuous improvement, good organization, and preparation.

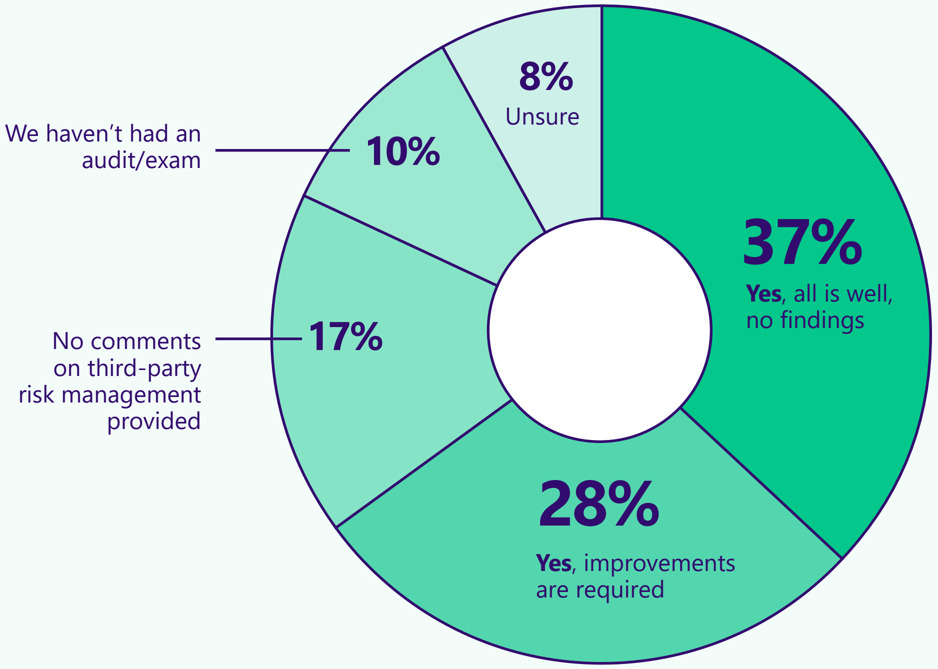
As a best practice to promote continuous improvement, third-party risk management programs should self-audit to identify gaps or areas of improvement.

When self-auditing your third-party risk management program, consider the following:

- 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.
- Do you have documented evidence that your processes are being followed and executed as expected?
- How effective are your processes and tools for identifying, assessing, managing, and monitoring risk?
- Are processes executed consistently?
- Is there clear accountability and oversight for third-party risk management activities and tasks?

If you discover issues or items needing attention, document them and begin working on a remediation plan. This approach is beneficial as it proves an understanding of third-party risk management best practices and regulatory requirements to your auditors/examiners. It also ensures issues are prioritized and managed before they become significant problems.

During your last exam/audit, did your regulator/auditors provide feedback on your current third-party risk management program?



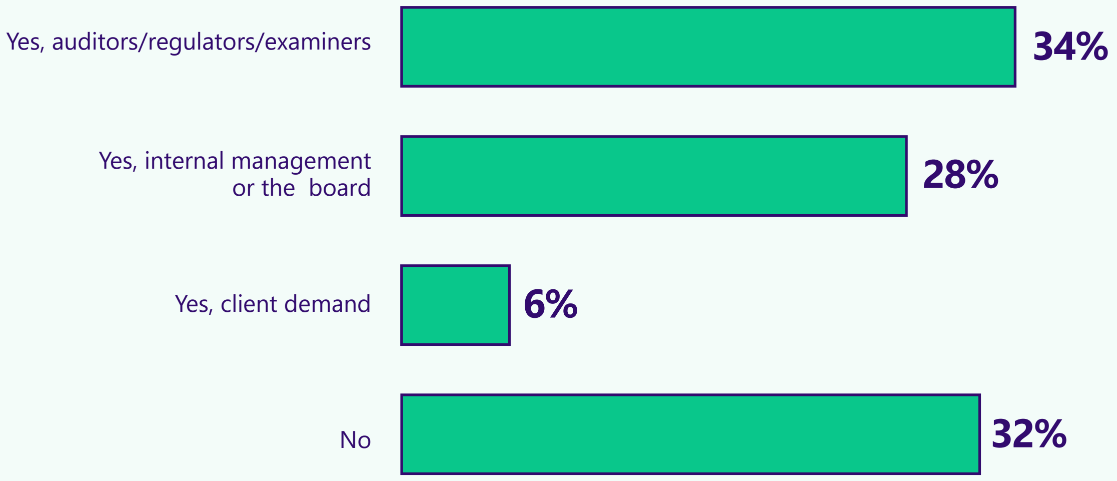
Pressures to Improve Third-Party Risk Management Programs

Third-party risk management is constantly evolving to address newly emerging risks. A fundamental goal of most third-party risk management programs is to ensure continuous improvement and meet regulatory requirements. Although the reasons behind this objective may vary depending on the organization and industry, the fact that the risk landscape is constantly shifting means that **neglecting to update and improve third-party risk management practices over time can lead to suboptimal risk management, costly mistakes, operational interruptions, and increased scrutiny from management, regulators, and the public.**

In the survey, we asked the participants whether they experienced pressure to enhance their third-party risk management programs or not. Out of all the respondents, 68% said they were. Twenty-eight percent (28%) said that their management and board of directors were urging them to improve, while 6% believed that client demand was the driving force behind this need for enhancement.

It's not surprising that 34% of respondents reported auditors and regulators as sources of pressure. Regulatory compliance is a crucial goal for most third-party risk management programs, and ongoing improvement efforts are often driven by new and changing regulations.

Are you feeling pressure to improve your third-party risk management program? If yes, what is the most significant source?



In 2023, a significant regulatory event occurred for many third-party risk management programs. The Interagency Guidance on Third-Party Relationships was released, which had been long-awaited. The guidance harmonized expectations between the Office of the Comptroller of Currency (OCC), Federal Deposit Insurance Corporation (FDIC), and the Federal Reserve System (Fed) for the first time. As a result, financial institutions subject to the oversight of these agencies now have the same requirements for managing third-party relationships.

The new guidance has clarified the definition of third party to include any business relationship (by contract or otherwise), which has resulted in a significant expansion of scope for most third-party risk management programs. Smaller financial institutions, such as community banks, now face significantly more prescriptive requirements than ever before.

Beyond the interagency guidance, new data breach notification rules, state privacy laws, and international data and privacy mandates have all served as motivators to improve processes in 2024.

Interestingly, 32% of organizations felt no pressure to improve their third-party risk management program. This may be because as program maturity increases, more organizations may be practicing proactive vs reactive continuous improvement to stay ahead of internal and external scrutiny.

Conversely, in some organizations, third-party risk management may receive less attention than it requires from management teams and boards. Without proper oversight, programs may stagnate and lack the motivation to enhance their processes.

One of the best ways to identify if your third-party risk management program needs improvement is to determine if it's reactive vs proactive. Here are some questions to ask:

- ? Does my organization's leadership team communicate the importance of third-party risk management, set expectations for both employees and vendors, and ensure there are adequate resources?
- ? Are there clear roles and responsibilities for managing vendor risks? Are employees and vendors held accountable for managing risks and performing responsibilities?
- ? Does my organization openly communicate and share information on vendor risks and what steps are being taken to manage those risks?
- ? Does my organization use policies, procedures, and standards to guide decision-making on third-party risk management activities? Is there oversight and controls to ensure the program is effective and compliant?

Emerging Third-Party Risks

Emerging Third-Party Risks

Top Concerns Ranked

It's common knowledge that identifying and managing new and emerging risks is a significant component of effective third-party risk management. Emerging risk concerns may vary depending on organization and industry. We asked which of the following risks survey respondents were most concerned about going into 2024.

Here are how our participants ranked the emerging risks:

1

Increase in cybersecurity attacks on vendors.

Cybersecurity is a major concern for organizations across industries, and for good reason. Cyberattacks and data breaches can happen to almost any organization, making it crucial to be prepared. Cybercriminals are becoming increasingly sophisticated, and they often target third-party vendors who may be more vulnerable. As these attacks become more complex and data breaches become more severe, the costs and resources required to address them also increase. One of the most common mistakes organizations make is focusing solely on protecting their own systems while failing to effectively verify and monitor the cybersecurity posture of their vendors.

Essential processes such as risk assessment, due diligence, and monitoring can minimize the occurrence and impact of third-party cyber incidents. However, for third-party risk management to be effective, it requires organizational and budget support from management, skilled people, well-designed processes, and effective tools.

Speaking of tools, as previously mentioned briefly, risk intelligence is a powerful one for assessing and monitoring vendor cybersecurity and is a great complement to any third-party risk management program. Nowadays, many companies offer products and services that not only supply risk reporting for a specific point in time, but also offer continuous real-time cyber risk monitoring.

Risk intelligence helps alert your organization if your vendor experiences a declining cybersecurity rating, doesn't meet technical compliance standards, or suffers a data breach. Although these services do come at a cost, they are often far more affordable than dealing with a single small-scale data breach. As the saying goes, "An ounce of prevention is worth a pound of cure."

2 Use of AI by vendors.

It's no wonder that AI hit the number two spot in this year's survey. Throughout the past year, the news was dominated by AI and its potential risks – particularly its impact on society and jobs. There were debates about the ethical implications of using AI, such as its potential to perpetuate biases or cause harm to individuals. The rise of deepfake technology also raised concerns about the potential for AI to spread misinformation and manipulate public opinion. Many were also worried about the possibility of job loss due to automation.

Third-party risk management practitioners face a number of added concerns when it comes to the risks associated with AI provided by third parties. These risks include data security, privacy, copyright infringement and intellectual property, algorithm transparency, regulatory implications, and more. Despite the fact that there are few regulatory guidelines and differing opinions on how to truly mitigate these AI risks, many third-party risk management programs are working hard to identify, assess, and manage them.

3 Pending or anticipated regulatory changes.

Regulatory compliance is one of the primary drivers of most third-party risk management programs. However, keeping up with changing regulatory requirements and guidelines can be challenging, particularly when the expected changes require an organization to significantly expand or change their third-party risk management processes and program.

Last year, several new and updated regulatory guidelines were released, including the Interagency Guidance for Third-Party Relationships, new cybersecurity disclosure rules from the SEC, and eight newly enacted state privacy laws, all of which kept third-party risk management programs very busy.

4 The availability of vendors in an unexpected event (continuity planning).

In recent years, vendor business continuity and resiliency has been a major concern for organizations, second only to vendor cybersecurity. However, this year it has slipped to fourth place, which is surprising. With the increasing threat of natural disasters, cyberattacks, and pandemics, organizations must continue to prioritize vendor business continuity.

CONSIDER THIS SCENARIO

If a critical supplier experiences considerable damage to their operations due to a natural disaster, your organization's operations could come to a standstill. This could lead to angry customers, frustrated employees, lost revenue, and damage to your reputation. Unfortunately, these scenarios do occur. To mitigate potential risks and ensure operational resiliency, it's essential to ensure your vendors have robust and tested business continuity plans.

5 Changes in a vendor's financial health.

Last year, the failure of three regional banks, high interest rates, tightening credit, record-breaking inflation, and massive layoffs reminded many organizations about the importance of their vendors' financial health.

Review and assess the financial stability of your vendors, especially those that pose a substantial risk or are critical to your operations. This can be done by regularly monitoring their financial reports and credit ratings. Keep an eye out for signs of financial instability such as missed payments, increased debt levels, declining sales, and a decrease in profitability. If you notice any of these warning signs, it's important to take action to minimize any potential risks.

6 Environmental, social, and governance (ESG) disclosure and reporting.

Love it or hate it, ESG disclosure and reporting is ranking the sixth top concern for our survey respondents. ESG remains a hot topic because it focuses on sustainability and ethical practices, which are increasingly important to consumers and investors. But it's not without its critics, which has caused it to be an issue under debate and stalled regulations. Despite this criticism, ESG doesn't appear to be going anywhere, and if anything, it's becoming more entrenched in business environments, both in the U.S. and abroad. For example, regulators in Europe and California have implemented ESG-related climate disclosure and accountability rules. The SEC is anticipated to release its own climate disclosure rules in April 2024.

The tug of war over ESG is certainly challenging for third-party risk management practitioners who have long been told to anticipate and prepare for vendor ESG transparency and reporting as part of due diligence and monitoring practices.

To avoid a start and stop approach, align third-party risk management programs with the ESG objectives and goals held by your organization and take appropriate actions. Even organizations without ESG initiatives may have to comply with specific requirements if proposed regulations, such as the SEC climate disclosure rule, come into effect. So, stay aware of proposed ESG-related regulations and rules.

7 Identifying and reporting the diverse status of vendors (supplier diversity).

As in the 2023 survey, supplier diversity is ranking lower on the list of third-party risk management concerns. Like ESG, the concept of supplier diversity isn't without its critics and champions in the private, public, and government sectors. Supplier diversity is still very relevant to organizations who are subject to specific regulations, including the Federal Acquisition Regulation (FAR), which requires supplier diversity programs from government contractors.

Other regulatory bodies, such as the FDIC, encourage financial institutions to incorporate supplier diversity into their policies and practices. Even when supplier diversity isn't a mandate, many organizations believe it's a business strategy that can encourage innovation, drive economic growth (especially for underserved communities), and enhance overall brand appeal.

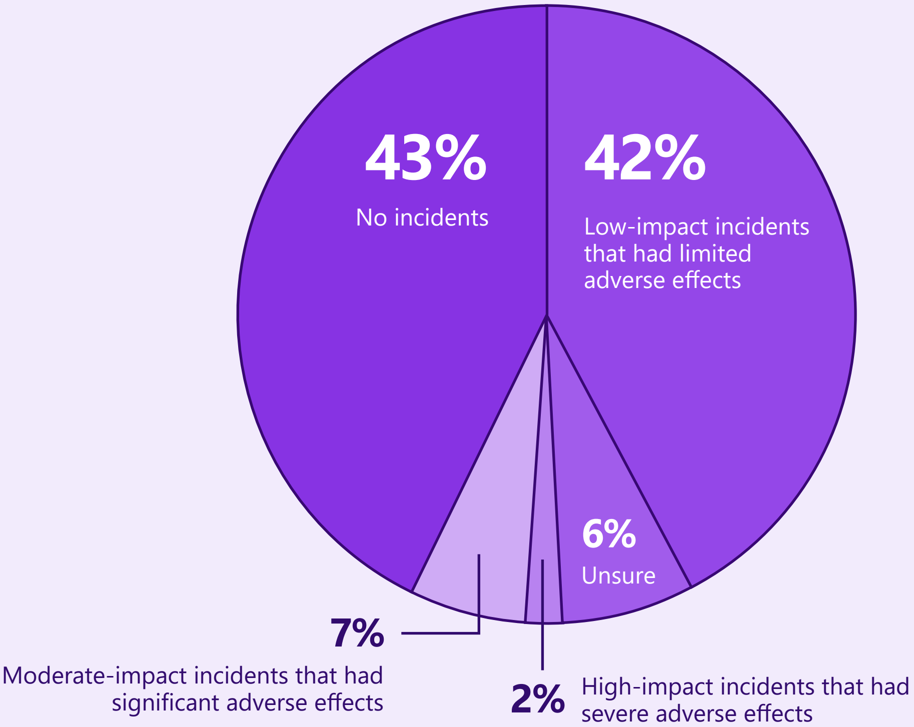
Cybersecurity Events

In most third-party risk management programs, cybersecurity is a top priority because it's the number one third-party risk. Organizations can't afford to be complacent in the face of increasing cyberattacks, data breaches, and ransomware resulting from third-party relationships. Questions were included in this year's survey to determine how organizations are being affected by cyber risk and what measures they're taking to combat vendor cybersecurity risks.

First, we asked how many organizations experienced a third-party cyber incident over the past year, and how significant the impact was. A positive finding is that 43% of respondents didn't report any cybersecurity incidents in the previous year. **Over half of respondents reported incidents, with varying degrees of impact.** Fortunately, in the majority of reported cases (42%), the impact of the incidents was limited. Even so, 7% sustained serious adverse effects as a result of these cyber incidents and 2% considered the impact to be severe.

These numbers are mostly consistent with last year's survey and demonstrate the continued need to aggressively identify, assess, monitor, and manage third-party cybersecurity risk.

Over the past 12 months, has your organization experienced a third-party cybersecurity incident?



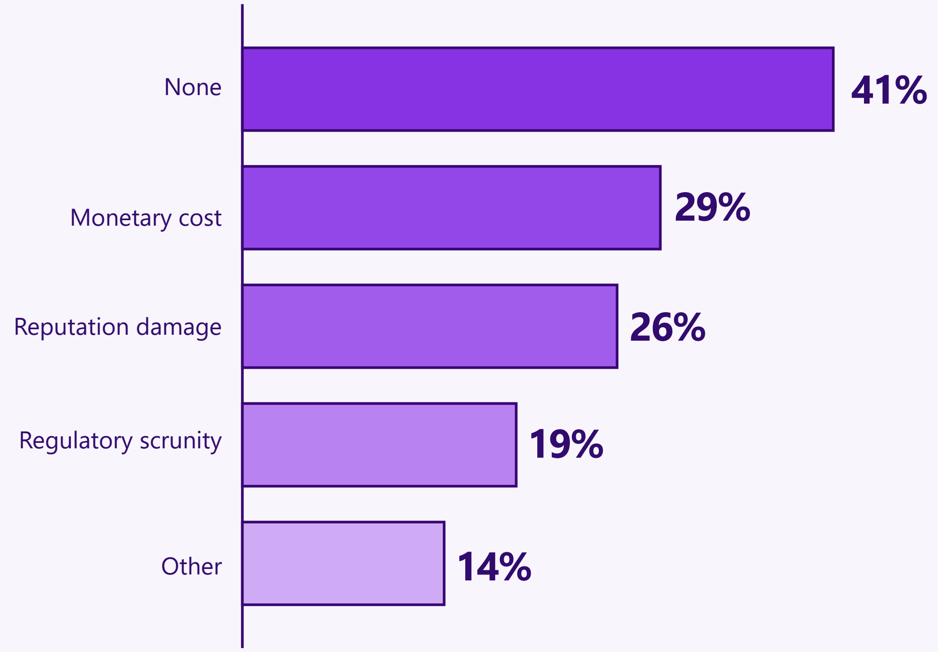
Third-Party Cyber Incident Impact

The impacts of a third-party cyber incident can be wide ranging and long lasting. It may include the financial cost and resources to remediate a data breach, operational interruption, regulatory fines and enforcement actions, and damage to an organization's reputation and brand. For those organizations that experienced a third-party cyber incident, we wanted to know the ways their organization was affected.

Remarkably, 41% of organizations reported no impacts, and it's unlikely that all of them were simply lucky. A well-designed process, good planning, and strong internal controls can often be credited with reducing or eliminating the potential impacts of a third-party cyber incident. For those that were impacted, monetary costs (29%) and reputation damage (26%) were reported. Another 19% of respondents cited regulatory scrutiny as an outcome of the incident, and 14% cited other impacts.

Third-party risk management practitioners can never ignore the fact that third-party cyber incidents can cause serious damage to their organization. However, effective risk assessments, due diligence, and ongoing risk monitoring can help you prevent or minimize third-party cyber risks.

What were the biggest impacts of the incident?
*Respondents were asked to select all that applied.



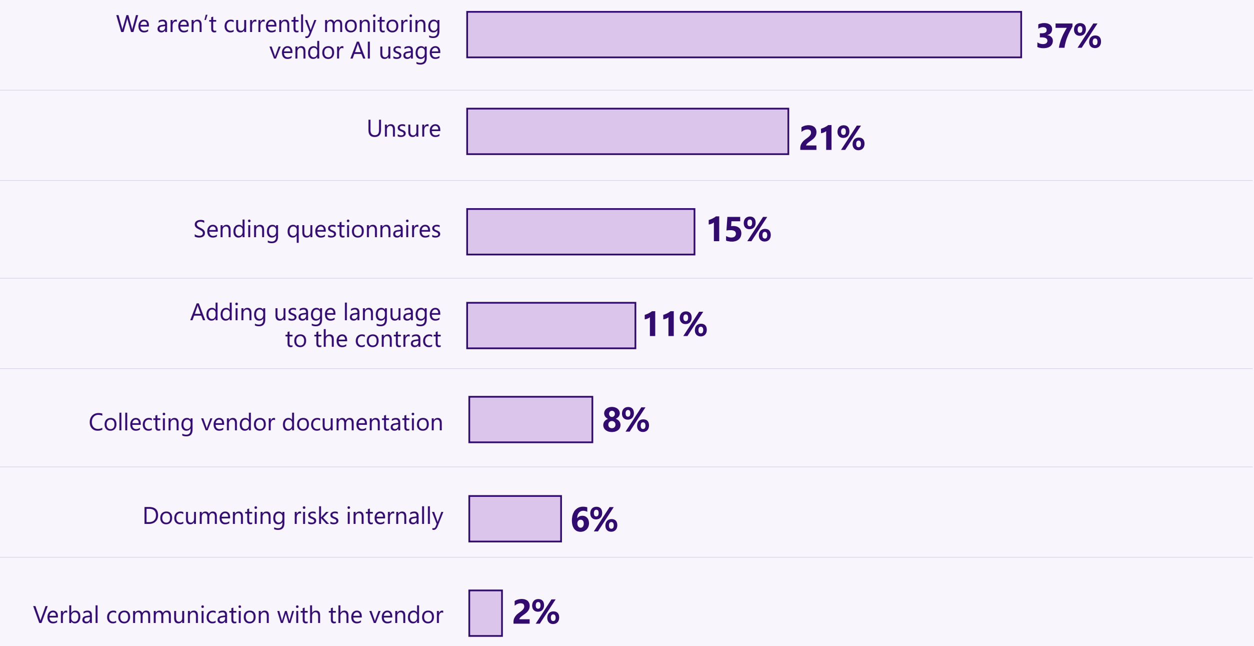
Artificial Intelligence (AI)

Participants ranked vendor AI risk as the second most important concern when it comes to new and emerging risks. It's no coincidence that AI is top of mind these days, as the focus on and discussions regarding AI dominated the news last year. As a result, businesses, governments, consumers, and users now have elevated awareness of concerns related to AI's ethical use, data security, accountability, and transparency and human rights implications.

Moreover, concerns about the ethical use of AI, as well as its potential dangers, have prompted the rapid development of regulations domestically and abroad. In the U.S., President Joe Biden's executive order on AI calls for more transparency and new standards, with nuanced approaches to regulating each sector independently. The National Institute of Standards and Technology (NIST) has already proposed a framework for sectors and agencies to follow. The European Union has recently adopted the AI Act, which sets new restrictions on AI use cases and mandates transparency from organizations. Assuming the EU completes the final procedures, the AI Act should become law sometime in early 2024.

As AI develops and concerns escalate, third-party risk management programs may find it challenging to identify, assess, and manage the real risks associated with vendor-provided AI. This year, we have added a new question to the survey to assess how organizations manage third-party AI risks. The results tell an interesting story.

How is your organization currently or planning to assess/ monitor vendor usage of artificial intelligence (AI)?



More than half of the responding organizations either didn't monitor vendor AI usage (37%) or were unsure if they did (21%). Despite the fact that third-party vendors have provided or used AI for many years, the realization of AI as yet another third-party risk has only recently begun to gain traction. For this reason, many organizations have not yet incorporated AI into their third-party risk management programs.

For organizations trying to identify, assess, and manage AI risks, 15% of participants use vendor risk questionnaires to gather information, and 8% are collecting vendor documentation. Eleven percent (11%) were adding specific language to their contracts, documenting the risk internally (6%), and having direct discussion with their vendors (2%).

As with most new and emerging risks, third-party risk management practitioners may need additional resources, such as qualified subject matter experts, to help define and assess AI risks as part of developing effective processes to manage them.

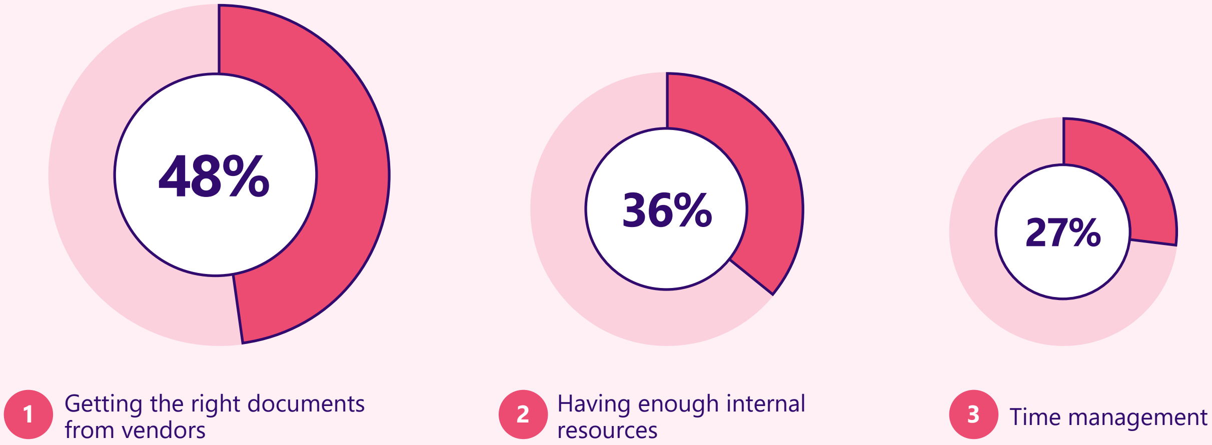
Organizations that don't have qualified AI subject matter experts in-house are strongly encouraged to seek external expertise and advice as necessary.

Third-Party Risk Management Challenges

Third-Party Risk Management Challenges

Our survey respondents were asked to identify the challenges they face in third-party risk management. We listed 20 areas of concern and asked them to rank their top three. Historically, the results have been consistent.

According to this year's survey, the top three challenges are:



*Respondents were asked to select all that applied out of a list of 20 options

Getting the Right Documents from Vendors

Over the past few years, participants have said that getting the right documents from their vendors is a big challenge. Nearly half believe it to be their top challenge this year. It raises the question of why it's so difficult and how we can improve it. Truthfully, if your third-party risk management document request doesn't include a list of standard documents to collect per risk domain, clear descriptions of those documents, and an articulated rationale for collecting them, vendors will often provide incomplete or inaccurate documentation.

Even with the best processes, vendors don't always return what's requested, or worse, they don't provide anything. So, how can third-party risk management programs reduce the number of documents they must chase down?

Here are some best practices and options to consider:

✓ **Work with your SMEs** to create a standardized list of documents to request per risk domain as well as a list of suitable alternatives.

✓ **Automate vendor documentation requests and tracking** through a dedicated third-party risk management platform. Ensure requests include a list of all required documents, by risk domain, as well as the rationale for asking for them. If alternatives are acceptable, specify what they are. All requests should be time-bound and clearly state that no work will begin until due diligence has been completed and that any missing or incomplete documents will delay contract execution.

✓ **Train your vendor owners** to discuss the due diligence process with all perspective vendors, including the need to complete a vendor risk questionnaire and return documentation as evidence of their risk management practices and controls. Educated vendor owners can help vet vendor questions and ensure the vendor understands the importance of supplying proper and current documentation as requested.

✓ **Hold your vendor owner accountable** for tracking down missing documentation from their vendor.

✓ **Don't ever begin work or sign a contract until due diligence** has been successfully completed.

✓ **Consider outsourcing the vendor documentation collection process.** Many professional third-party risk management firms offer vendor document collection services, which is a time-intensive but largely administrative task. Outsourcing this process can return much needed bandwidth back to smaller third-party risk management teams, remove the frustration of chasing down missing vendor documents, and allow third-party risk management team members to focus on managing risks.

Having Enough Internal Resources

Third-party risk management teams are often very lean, which is a problem for survey respondents. Not having enough internal resources ranks second as a top third-party risk management challenge. The lack of internal resources can go beyond just the third-party risk management team.

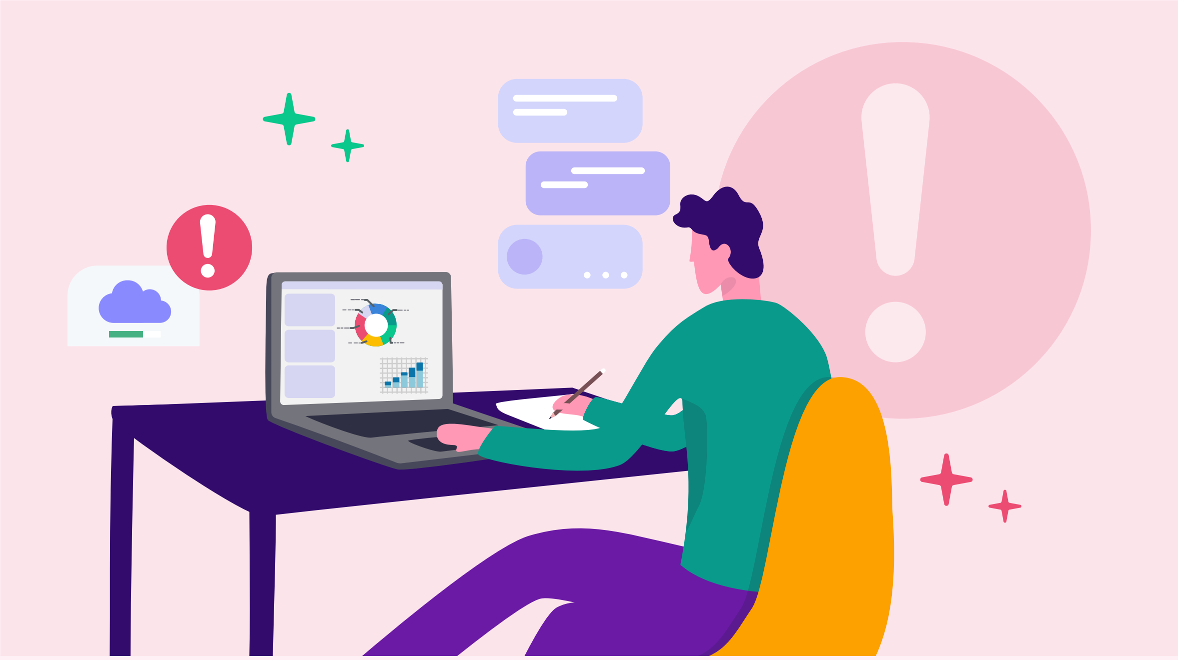
Internal subject matter experts often serve multiple functions and have competing priorities, which can mean vendor risk reviews are delayed or left undone. Vendor owners, feeling the pressure of meeting the expectations of their primary roles, may not produce quality or timely third-party risk management deliverables. Insufficient budgets and technology investments often mean third-party risk management teams are forced to use manual and error-prone methods and tools to manage their processes.

Too few dedicated third-party risk management team members can result in key risks being overlooked or addressed too late.

No matter where the shortfall is in the organization, it's important to remember senior management and the board are accountable for ensuring there are adequate resources for third-party risk management to be executed efficiently and effectively at the organization. Most regulators are specific in their expectation for management and the board to ensure proper organizational structures and staffing (level and expertise) to support third-party risk management processes.

Beyond adding full-time employees, it's possible for organizations to implement different resourcing strategies to ensure third-party risk management is effective and efficient, such as:

- ✓ **Utilizing dedicated third-party risk management software**, which can enable automation, reduce errors, promote accountability through transparency and reporting, and enhance communication and collaboration both internally and with vendors. Most third-party risk management software and systems have been specifically designed to manage the many complex and interdependent processes associated with third-party risk management and help teams do more with less.
- ✓ **Defining clear roles and responsibilities** ensures individuals and teams are held accountable for their various tasks across the organization and reduces or eliminates the "not my job" mentality that often results in work that isn't completed or is poor quality.
- ✓ **Outsourcing portions of third-party risk management** can be a practical option when an organization lacks enough internal resources or expertise. From outsourcing vendor document collection to using external, certified subject matter experts to conduct vendor risk reviews, outsourcing can be a viable and often affordable way to supplement resources, improve effectiveness, and ensure processes are happening on time.



Time Management

Coming in third on the list of top challenges is time management. Third-party risk management teams never have enough time in the day to get it all done. As a result, every day is an exercise in reprioritizing tasks and activities.

Too much work and too few resources is only one of the reasons time management is a top challenge for teams. Ineffective processes, errors, and rework resulting from outdated, manual, and error-prone processes can also be to blame.

Low organizational compliance and pushback from vendor owners and business units are yet another reason third-party risk management practitioners may be feeling crunched.

Even the most experienced and effective teams can struggle with time management. While solutions like automating processes through dedicated third-party risk management software platforms are definitely recommended, there are some other often overlooked strategies that can help:

- **Invest in training.** Third-party risk management teams that provide comprehensive training to vendor owners, business line management, and other stakeholders end up spending less time answering the same questions and can more reliably depend on others outside of the team to effectively complete third-party risk management tasks on time and at the right level of quality. When there is high third-party risk management competence in an organization, teams can focus their efforts on where they're needed most.

- **Set expectations and communicate.** A vendor owner who is anxious to onboard their new moderate-risk vendor is likely not aware of the other vendors already in the queue or the critical vendor's performance issues that require third-party risk management's immediate attention. For practical reasons, most third-party risk management processes can't operate solely on a first-in-first-out queue system. By setting and communicating reasonable expectations with internal customers and stakeholders and helping them understand the necessity of a risk-based approach, they will be better able to plan their activities, reducing the number of inquiries and "emergencies" landing on third-party risk management's desk.

Establish third-party risk management work routines and hold time for them on your calendar. One of the biggest reasons third-party risk management teams face time management challenges is related to the number of rapid-fire requests and one-off demands they must address every day. Constantly juggling so many tasks means that some are more or less permanently deprioritized and never get done, which just adds more stress. An alternative approach is dedicating a specific amount of time for regular third-party risk management work each week.

EXAMPLE

Instead of reviewing every new inherent risk assessment the moment it hits your inbox, reserve 30 minutes on Monday, Wednesday, and Friday mornings to review and respond to these assessments. Similarly, you can reserve a block of an hour or two once or twice a week to go through due diligence results, performance monitoring, etc.

The key to doing this effectively is to clearly set expectations for when stakeholders should reasonably expect a response or an approval and stick to it. This approach not only allows third-party risk management practitioners to take more control over their responsibilities, but over time it's possible to really quantify the actual time and effort it takes to keep third-party risk management moving, which can be very useful if you need to justify a request for additional resources.

While we have only addressed the top three challenges in detail, **completing risk assessments** and **automating processes** were other top concerns. Broadly speaking, many common third-party risk management challenges can be attributed to a lack of resources, internal expertise, or organizational support. When teams are fully resourced and supported, they're better enabled to address challenges more effectively and efficiently.

Third-Party Risk Management Value and Benefits

Third-Party Risk Management Value and Benefits

Return on Investment

There are many factors that go into an organization's decision to invest in third-party risk management. Organizations who receive benefits and a return on investment (ROI) tend to be more committed to third-party risk management as a practice. According to our survey, an overwhelming 96% of respondents said their organization believes there is ROI for third-party risk management activities.

Of the cumulative 96%, 40% said there may be differing opinions at their organization. In many organizations, the actual ROI of third-party risk management has yet to be clearly measured or expressed in terms of hard dollars. Additionally, when third-party risk management is seen as purely a regulatory requirement or "necessary evil," there may be little analysis of its true value.

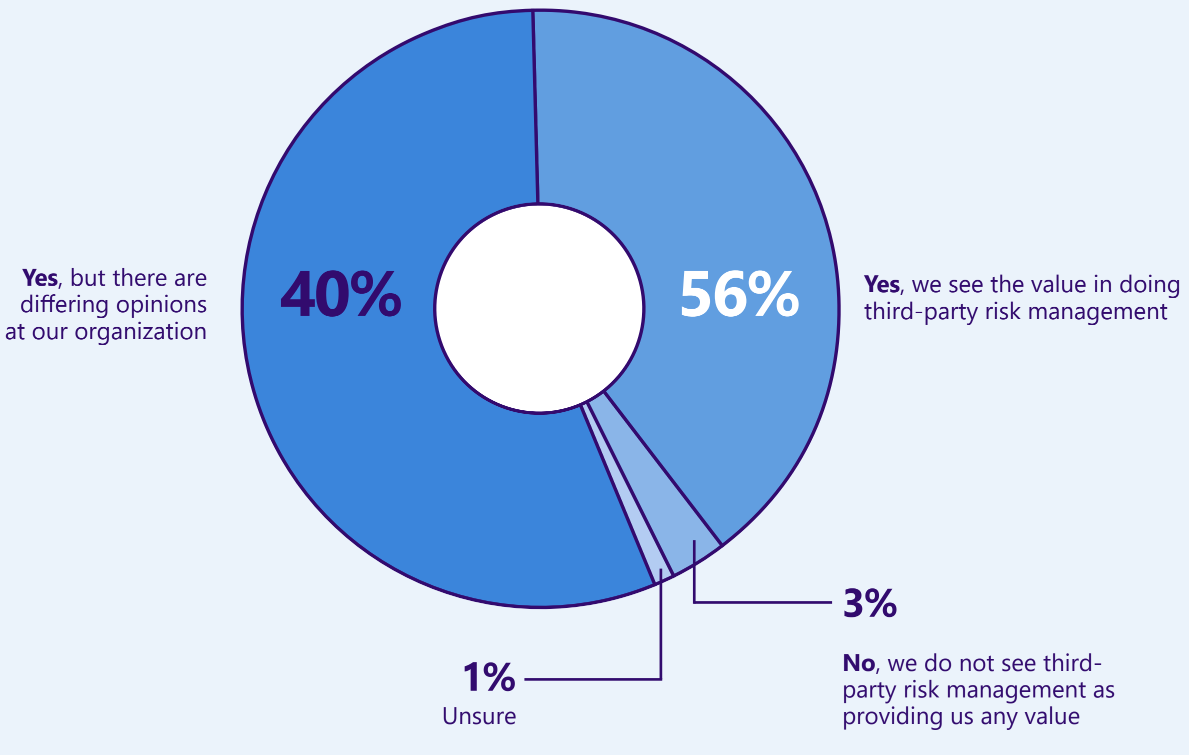
Third-party risk identification and effective risk management provides more benefits than regulatory compliance alone.

By enhancing contract management, improving third-party service levels, and identifying and managing vendor risk issues before they become material, a well-executed third-party risk management program often helps organizations avoid unexpected expenses such as litigation costs, regulatory fines, rework, lost productivity, and negative customer perceptions.

If an organization wants to quantify third-party risk management's ROI, it needs to be able to articulate the benefits beyond compliance and think about the potential impacts of unmanaged third-party risks.

Often, this requires an organization to shift its culture away from practices that only consider dollar savings or revenue when calculating ROI. While it's possible to estimate the impact and cost of many unmanaged third-party risks and translate them into cost-avoidance calculations, some may argue assigning a value to cost avoidance isn't practical. Still, there's no denying the potential impacts to an organization if third-party risk management isn't implemented or performed correctly.

Does your organization believe there is a return on investment (ROI)/value from investing in third-party risk management activities?



EXAMPLE

Data breaches are a perfect example. Third-party risk management is instrumental in identifying, assessing, and verifying vendor cybersecurity risk management practices, controls, and practices, and continuously monitoring their cybersecurity risk profile. Without these essential practices, the likelihood, occurrence, severity, and impact of third-party data breaches grow exponentially. So, just how bad can it get? What could a single breach cost your organization?

For every vendor that has access to an organization's (or its customer's) sensitive data, there are potential breaches. Per the latest IBM Ponemon Institute's Cost of a Data Breach report, the average cost of a data breach reached an all-time high in 2023 of $4.45 million with an average cost of $165 for each compromised record. Assume your organization has ten vendors with access to 20,000 records of sensitive data. Let's say that just one vendor experiences a breach, which could easily translate into $3.3 million of unplanned expense. That's just the breach remediation cost, it doesn't include the potential for lost customers or damage to your reputation.

Even if cybersecurity is a more obvious example, the cost of regulatory noncompliance shouldn't be ignored. In 2023, a major financial institution was fined a record-breaking $15 million by the OCC. The fine was levied as an enforcement action on the bank for failing to properly govern and oversee a third-party affiliate who didn't have proper call monitoring controls or appropriate mechanisms to document and track customer complaints.

Considering the number of vendors most organizations utilize, the value of third-party risk management can be exponential, as the average organization can lose millions just through a single incident of unmanaged third-party risk. If it helps, you might visualize third-party risk management as the seatbelt on your car. True, no one is particularly enthusiastic about it, but it's essential. Anyone who's ever been in even a mild accident can attest to the importance of wearing one. Third-party risk management serves a similar purpose in that it can help avoid or prevent serious harm to your organization. The expense of third-party risk management is miniscule compared to the financial, regulatory, and reputation damage an organization may experience without it.

Benefits

As part of our annual survey, we asked respondents to rank their organization's primary reasons for having a third-party risk management program. These rankings are consistent with other elements of our survey and are as follows:

Rank 1 to 6 your primary reasons for doing third-party risk management.

1. Meet regulatory requirements to avoid costly fines and legal repercussions
2. Avoid third-party cyber incidents
3. Protect our brand and reputation
4. Align with industry best practices and standards
5. Managing vendor performance
6. Controlling vendor costs (negotiations, avoiding auto-renewals)

As in previous surveys, regulatory compliance remains the number one reason why organizations perform third-party risk management. Meeting the regulators' expectations may be the primary driver, but compliance doesn't wholly encapsulate the many objectives of third-party risk management.

Avoiding third-party cybersecurity incidents, protecting your brand and reputation, and ensuring vendors are providing the anticipated value at the agreed-upon price for the products and services they provide are important.

What primary benefit(s) do you believe third-party risk management gives your organization?

While we have reiterated the many reasons why organizations should have third-party risk management programs, we asked our survey participants to tell us in their own words about the benefits of third-party risk management. We've highlighted some of the answers below:

Our customers, shareholders, and regulators depend on us to make sure we're making risk informed decisions and acting in their best interest.
Wealth/Asset Management, 5,000+ employees

Visibility into the entirety of the vendor lifecycle, regulatory protections, and protections from the inevitable challenges that come with dealing with vendor relationships.
Bank, Greater than $10B

Essential for the discovery of nonconformance and noncompliance issues, evidence, policies and processes prior to the annual ISO recertification audit(s).
Railroad Transportation, 1-100 employees

Peace of mind that our third parties are being reviewed/ monitored for risks and we understand how those risk can impact our organization.
Credit Union, $1B to $10B

Controls, evaluation, and process to select third-party providers.
Fintech, 251-500 employees

A third-party risk management program guarantees confidence and judgment to the business when acquiring new services with third parties, allowing compliance with the required security posture.
Credit Union, Less than $1B

Third-party risk management significantly enhances our organization's resilience against external threats and vulnerabilities, safeguarding our operational integrity and reputation. It also fosters stronger, more transparent relationships with vendors, ensuring compliance and aligning their performance with our strategic objectives.
Retail, 5,000+ employees

Governance, better control of third-party spend, and reduces the risk of third-party incidents.
Insurance, 1,001-5,000 employees

Enables the organization to mitigate potential reputational risks, alleviates duplicating payments for the same service, and effective contract management and negotiation. Contributes to effective business continuity strategies.
Brokerage, 1-100 employees

Peace of mind, savings through contract management, and being compliant with regulatory requirements.
Bank, Greater than $10B

Assurance our partners can successfully protect our borrowers' information.
Mortgage, 251-500 employees

Decreased risk of litigation by clients.
Consulting, 1,001-5,000 employees

Centralized and comprehensive view of risk related to our thousands of third parties.
Consulting, 5,000+ employees

Raising awareness to the business on the possible risk associated with any vendor engagement.
Non-Financial Institution Lending, 501-1,000 employees

We outsource the majority of our banking applications, so third-party risk management is vital to ensure that those providers are maintaining a secure environment to protect the confidentiality, integrity, and availability of data and applications.
Bank, $1B to $10B

Part of a suite of services offered to our clients. Both good business and corporate governance.
Consulting, 1-100 employees

Understanding our threat landscape by the risk that is introduced by the use of third parties.
Manufacturing, 5,000+ employees

Better cyber posture, risk, and vulnerability assessments.
Oil/Gas/Energy, 501-1,000 employees

Better risk management and the ability to address issues in a timely manner, especially during an incident such as a cyberattack at the third party.
Bank, $1B to $10B

Proactively identifying and taking steps to mitigate potential risk associated with third-party vendors either before or after onboarding.
Retail, 5,000+ employees

Reduce risk and adhere to laws, regulations, and standards.
Hospitality, 101-250 employees

We can categorize third parties to have a clear understanding of how they engage with our company and can determine the level of trustworthiness of their program.
Insurance, 5,000+ employees

It helps us with monitoring our vendors, our contracts, and the risks associated. It also provides transparency for audits, as well as assessing the health of our vendors/vendor relationships.
Bank, $1B to $10B

Maintaining a centralized inventory of our vendors and contracts and utilizing software and technology to measure and mitigate vendor risk, including cyber and data security mitigation. Utilizing software to monitor vendor performance.
Bank, Greater than $10B

Being able to evaluate a vendor's ability to meet the needs of our organization and protect the data and interests of our members and company.
Credit Union, Greater than $10B

Increased client satisfaction that we're doing our due diligence, proactive risk management for sustainability, preventing breaches and security risks, and being able to make more informed decisions.
Technology Services or Software, 1-100 employees

Understanding the risks and controls for each vendor up front allows our organization to decide if they want to do business with the vendor before entering into a contract.
Credit Union, Greater than $10B

Helps achieve compliance with data privacy laws and regulations, as well as provides legal protections for definition of liability for cyber incidents and other unfortunate events which may occur during the course of business.
Legal, Less than $10B

The current environment in which we all work/exist has significant regulatory oversight over third-party risk management. It ensures we stay in compliance and are audit ready at all times.
Bank, Less than $1B

Holistic approach to compliance and risk management for the entire information and communications technology value chain.
Oil/Gas/Energy, 5,000+ employees

Prevent/manage data loss from third-party vendors.
Healthcare, 5,000+ employees

Third-party risk management helps to ensure that the firm is protected and prepared for the risks of third parties accessing and storing our firm and client data.
Wealth/Asset Management, 101-250 employees

Provides a framework for onboarding, monitoring, and offboarding vendors. From actively monitoring vendors, it helps to build strategic partnerships with them.
Insurance, 501-1,000 employees

Gives us the ability to mitigate or at least remediate risk.
Consulting, 5,000+ employees

Our third-party risk management helps our company automate processes, such as tracking key dates and contract terms, due diligence collection, and ongoing monitoring activities.
Wealth/Asset Management, 251-500 employees

Oversight for critical parts of our business that are too expensive to handle ourselves.
Wealth/Asset Management, 101-250 employees

Our third-party risk management helps our company automate processes, such as tracking key dates and contract terms, due diligence collection, and ongoing monitoring activities.
Wealth/Asset Management, 251-500 employees

Third-party risk management gives the business a clear view of the amount of risk they will be taking on by using a certain vendor.
Insurance, 5,000+ employees

The framework to ensure third parties are abiding by contractual requirements and operating in a safe and sound manner to help our business achieve their goals.
Mortgage, 501-1,000 employees

Onboarding structure, risks, stratification, offboarding, vendor activation, risk reporting, risk partner information gathering, and sharing.
Healthcare, 1,001-5,000 employees

Ensures that potential vendors meet our local, state, and federal standards, policies, procedures, regulations, cybersecurity measures, corporate culture, and financial stability to reduce the risk of disruptive outages, downtime, disasters, and financial ramifications.
Consulting, 1-100 employees

Transparency into third-party risks, tools to inform decision-making, and tools to strengthen our risk posture and mitigate potential risk.
Insurance, 5,000+ employees

Control auto renewals, ensure contracts have applicable language, risk reviews.
Credit Union, $1B to $10B

Manage spend and risk and cover us with our clients and cover us with our regulators.
Wealth/Asset Management, 101-250 employees

Mitigation of risk and managing the vendors. Also making sure that we are aligned and associated with the best vendors.
Automotives, 5,000+ employees

A consistent and coordinated approach to managing third-party relationships and the risks associated with them.
Insurance, 501-1,001 employees

Formal assessment of vendor risk prior to contract and ongoing monitoring. A coordinated approach to managing third-party relationships and the risks associated with them.
Insurance, 501-1,001 employees

Identifies the potential risks vendors or suppliers present along the entire supply chain. It provides a comprehensive threat that the organization faces with their vendors.
Technology Services or Software, 1-100 employees

Meets regulatory obligations and protects the organization.
Retail, 5,000+ employees

Visibility into manageable or preventable risk.
Manufacturing, 5,000+ employees

Protecting our customer PII/PCI data.
Retail, 1,001-5,000 employees

Peace of mind regarding information assets' integrity, as well as compliance with customers' requirements.
Consulting, 101-250 employees

Protect the company against unnecessary risks.
Manufacturing, 5,000+ employees

Insight into risks associated with the use of third parties, which third parties access/store our data, and which third parties are critical to our business.
Mortgage, 5,000+ employees

Monitoring of a growing third-party population.
Bank, Greater than $10B

Ability to recognize and proactively respond to risks that may impact operational resiliency, financial reporting, information security, and reputation.
Insurance, 5,000+ employees

Vendor/third-party identification/risk ranking.
Government, 501-1,000 employees

Monitoring and reporting of our risk for regulators.
Bank, Less than $1B

Managing vendor risk and making sure our vendors are compliant with regulations and protecting consumer/customer data.
Wealth/Asset Management, 501-1,000 employees

Knowing WHERE our risks are, specifically sensitive data.
Credit Union, $1B to $10B

Regulatory conformance, clarity into relationship, and money savings by identifying duplicated contracts or outdated contracts that may be auto-renewing without awareness.
Mortgage, 251-500 employees

External oversight, best practices, regular monitoring.
Nonprofit, 101-250 employees

A central place where vendors are managed under a uniformed process.
Real Estate, 501-1,000 employees

Formal assessment of vendor risk prior to contract and ongoing monitoring.
Transportation, 5,000+ employees

Oversight and governance of vendors and fourth parties.
Technology Services or Software, 5,000+ employees

It helps to mitigate risk and helps to ensure compliance with regulators.
Fintech, 1-100 employees

Mitigate supply chain disruption to operations and risks.
Healthcare, 5,000+ employees

Risk protection to the company, as almost two-thirds of our work is done by staff at third parties.
Insurance, 5,000+ employees

Annual oversight into critical and material vendors' financial and security levels.
Credit Union, $1B to $10B

Third-party risk management safeguards our credit union from avoidable losses.
Credit Union, $1B to $10B

Client retention/growth, reputation management, and regulatory compliance.
Consulting, $1B to $10B

Greater assurance and insight into potential risks posed by vendors and suppliers.
Government, 251-500 employees

Oversight and management of supply chain risks.
Fintech, 1,001-5,000 employees

Minimizes the risk of a data breach.
Technology Services or Software, 501-1,000 employees

An overview of our vendors and their external risks, an overview of the internal risks (Compliance, Reputational, Financial, etc.), and advice on risk remediation.
Healthcare, 1,001-5,000 employees

Visibility to return on investment and control assurance.
Insurance, 1,001-5,000 employees

Promotes strong risk management practices of those we do business with. Reduces potential for cyberattacks.
Insurance, 5,000+ employees

Evaluating third-party vendors allows us to work with vendors that are diligent in protecting customer information with the same standards we use.
Bank, Less than $1B

Managing the company's risk exposure.
Retail, 5,000+ employees

Better knowledge of our vendors and the risks associated with using them. It also identifies our critical vendors from different aspects.
Insurance, 501-1,000 employees

Understanding the risks inherent in using third parties in order to manage those risks.
Fintech, 251-500 employees

Provides a more robust evaluation of our vendors prior to onboarding.
Technology Services or Software, 1,001-5,000 employees

Insight into the status of partners.
Real Estate, 251-500 employees

There are so many benefits.
Construction, 1-100 employees

Identify the security posture for third parties.
Insurance, 1,001-5,000 employees

Uncovering issues with vendors before the problem escalates and financial savings.
Healthcare, 251-500 employees

Proactive risk identification and management, raise awareness of our reliance on third parties, and the risks associated with that reliance.
Bank, Greater than $10B

Control of the threat landscape.
Education, 5,000+ employees

Recommendations and Best Practices

Recommendations and Best Practices

No matter your organization's size or industry, third-party risk management is becoming more urgent and continues to be essential. You need to keep your ears and eyes open for new and emerging risks, seek out and implement best practices, and stay alert to regulatory requirements for your industry.

You can always improve your program no matter how mature it may be. Take the time to review your program to identify any gaps or weaknesses, prioritize areas that can be improved, and document your plans to implement them. As we continue through 2024, here are some third-party risk management best practices to consider:

Best Practices for 2024

1. Ensure third-party risk management teams are **adequately staffed with skilled and experienced people.**
2. **Develop well-documented and current governance documents** such as a policy, program, and procedures.
3. Keep all assessments, questionnaires, and due diligence document requirements **up to date and relevant to the current risk environment**.
4. **Measure the impact of third-party risk management** through program metrics and reviews.
5. **Log, track, and monitor all vendor issues** until they're remediated.
6. **Educate vendor owners and management** on the purpose and objectives of third-party risk management. Train them to accomplish the tasks to fulfill their responsibilities.
7. Think about **other tools and strategies** that can help you work more effectively and efficiently like dedicated third-party risk management software and outsourcing low-value high-effort administrative tasks like vendor document collection.
8. Keep **senior management and the board well informed.**
9. Stay on top of the **industry news and enforcement actions.**
10. Keep a mindset of **continuous improvement.**

About Venminder

Third-party risk management done right.

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.

The Venminder platform is used by more than 1,200 customers across a wide range of industries to efficiently execute their third-party risk management programs. As Venminder's solutions are designed to accommodate growth and various levels of program maturity, customers range in size from small to top Fortune 100 organizations.

Our offerings.

Software Platform

Control Assessments

Managed Services

Request a Demo

Connect with us.

LinkedIn

X

Facebook

Stay updated on Venminder and third-party risk management.

- Attend a **live webinar**
- Get the **weekly Third Party Thursday Newsletter**
- Join the **Third Party ThinkTank Community**
- Listen to **industry interviews**
- Read the **latest articles**
- Download **free educational content**

SOURCES:

Federal Register. (June 9, 2023). Interagency Guidance on Third-Party Relationships: Risk Management. Federal Register. https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management

IBM. (2023). Cost of a Data Breach Report 2023. IBM. https://www.ibm.com/reports/data-breach

OCC. (July 25, 2023). OCC Assesses $15 Million Civil Money Penalty Against American Express National Bank Related to Bank's Governance and Oversight of Third-Party Affiliate. OCC. https://www.occ.treas.gov/news-issuances/news-releases/2023/nr-occ-2023-78.html

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.