venminder

State of Third-Party Risk Management

2023 Whitepaper

Table of Contents

03 **Executive Summary**

05 **Survey Highlights**

06 **Survey Results**

07 **Commitment to Third-Party Risk Management**
Dedicated Third-Party Risk Management Resources
Organizational Structure
Sponsorship from the Top
Program Investment

14 **Third-Party Risk Management Processes**
Size and Makeup of Vendor Landscape
Operating Models
Technology Tools Used

20 **Best Practices in Third-Party Risk Management**
Vendor Criticality
Inherent Risk Assessments
Residual Risk Assessment
Risk Re-Assessment and Due Diligence
Current Policy
Updated Inherent Risk Assessments
Updated Vendor Due Diligence Questionnaires and Documentation Requirements

27 **Third-Party Risk Management Growth and Pressures**
Maturity of Third-Party Risk Management Programs
Third-Party Risk Management Program Metrics
Regulatory Focus and Exams/Audit Results
Pressures to Improve Third-Party Risk Management Programs
Regulatory Scrutiny

35 **New and Emerging Vendor Risk**
Emerging Concerns
Cybersecurity
Supply Chain
ESG (Environmental, Social, and Governance)
Vendor Diversity

45 **Third-Party Risk Management Challenges and Ways to Advance Your Program**
Third-Party Risk Management Challenges
Training and Education
Outsourcing Third-Party Risk Management

50 **ROI and Primary Benefits**
Return on Investment
Benefits

59 **Recommendations & Best Practices**

60 **About Venminder**

Executive Summary

Venminder's State of Third-Party Risk Management 2023 survey provides insight into how organizations manage third-party risk today.

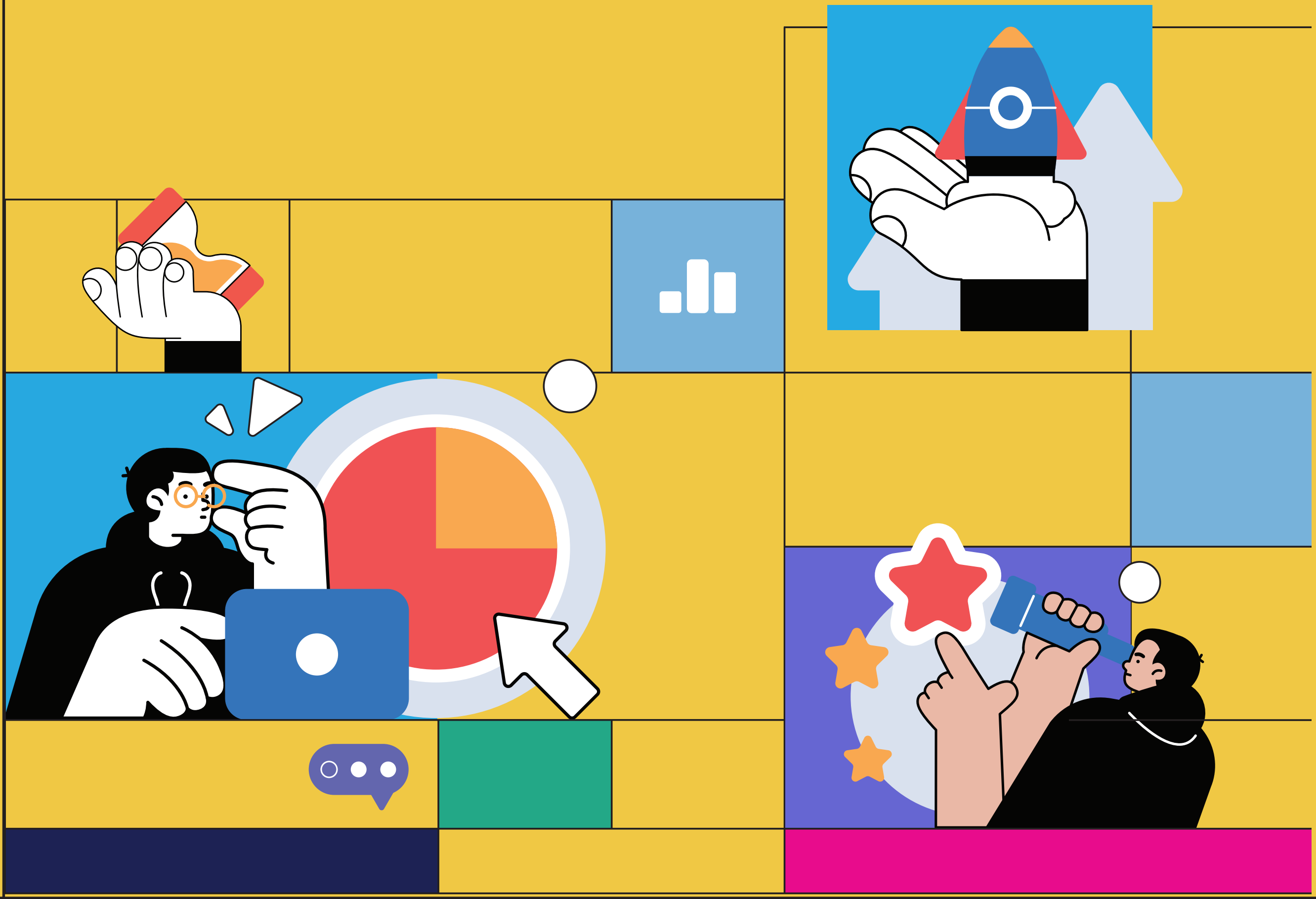
Results from the survey provide an in-depth look at current practices, challenges, compliance incentives, and third-party risk management benefits. For our seventh annual survey, Venminder surveyed individuals from a wide variety of organizations and industries, including financial services, fintech, 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 2022 through January 2023. Participants were allowed to provide anonymous, confidential answers to ensure the authenticity of their responses.

2022 was another year that emphasized the importance of third-party risk management on a domestic and international level. Cybercrime and attacks increased in record numbers, with healthcare and financial services sectors being hit the hardest. High fuel costs and labor shortages continued, resulting in ongoing supply chain disruptions around the globe. Geopolitical events such as the Russian-Ukrainian war resulted in increased government sanctions, and regulators enacted new laws to prevent human rights and labor abuses. Inflation rose to the highest level in 30 years, putting additional strain on an already troubled economy. As a result of these conditions and events, third-party risk management practitioners have been under increased pressure to identify, manage, and monitor new and emerging risks in virtually every industry and organization.

We can safely say that third-party risk management is more important today than ever and will become even more important tomorrow. While third-party risk management is a well-established practice, it is also a constantly evolving one. Organizations of all sizes and industries must continually adapt and change to effectively identify, assess, manage, and monitor vendor risks. By reviewing and analyzing the third-party risk management landscape and practices captured in our survey, organizations can see where they stand in relation to their peers and consider that information as they prepare for the future.

We would like to thank our 2023 survey respondents who generously shared their knowledge and experiences, as they provided valuable insights into real-world third-party risk management challenges and opportunities.



Survey Highlights

This year's Venminder State of Third-Party Risk Management 2023 survey offers insights for peer-to-peer learning and benchmarking against current best practices.

Here are just a few survey highlights:

1

Third-party risk management program metrics *are on the rise*

2

Cybersecurity *is still the #1 concern in TPRM programs*

3

Third-party risk management is helping organizations avoid ***supply chain*** *disruptions*

4

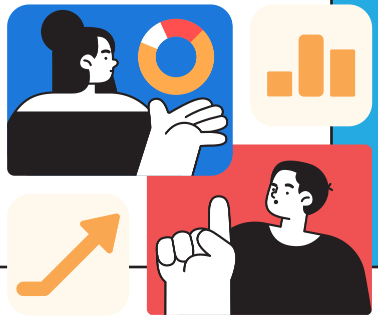
The majority of programs use ***dedicated third-party risk management platforms***

5

Vendor ***business continuity (BC) planning*** *is a major priority*

6

Outsourcing *is viable, but an underused option*



Survey Results

Commitment to Third-Party Risk Management

Commitment to Third-Party Risk Management

Dedicated Third-Party Risk Management Resources

A strong commitment to third-party risk management is the baseline requirement for a successful program. Adequate investments in human and financial resources are essential. Third-party risk management must have a reporting structure that supports, enhances, and aligns with its risk management purpose. Most importantly, it is the role of senior management to set an intentional "tone-from-the-top" to establish third-party risk management as an organizational priority. An organization's commitment to third-party risk management can be measured by these factors and others.

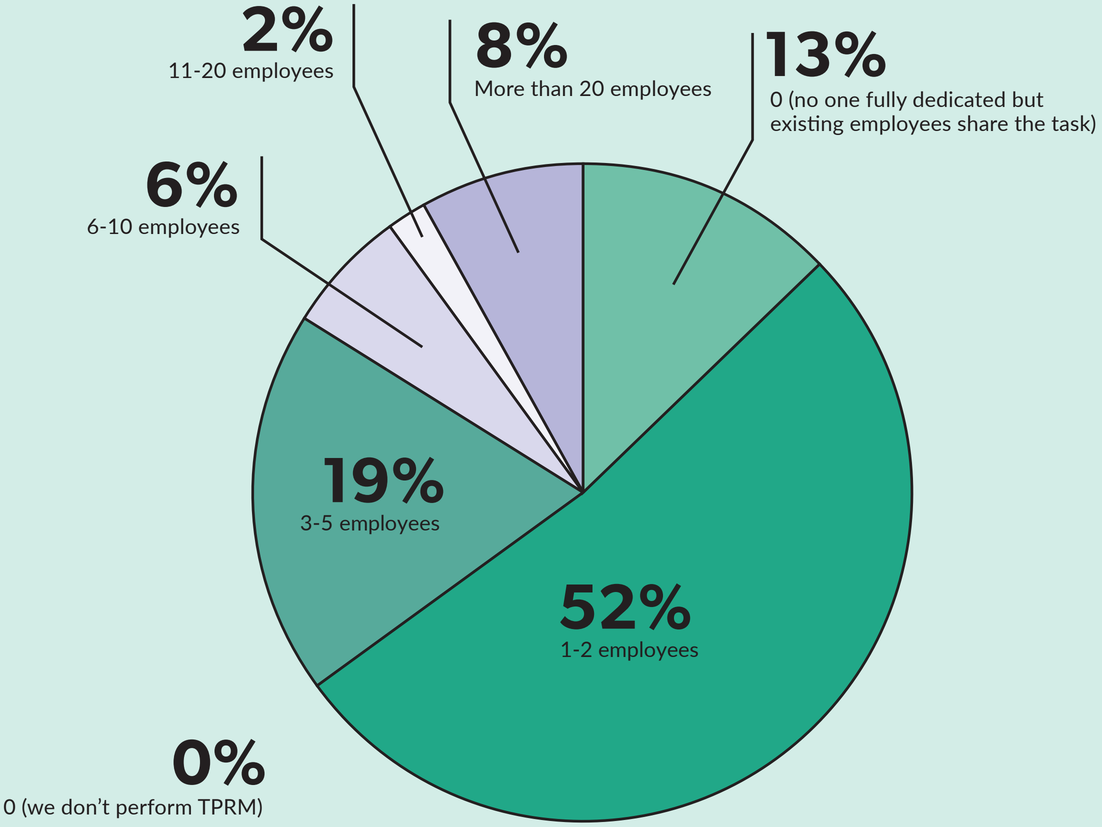
For third-party risk management to be successful, it must be sufficiently staffed with qualified personnel. Numerous factors influence the number of dedicated employees needed for a third-party risk management program. Automated third-party risk management programs, engaged vendors, and effective processes enable mature programs to achieve greater efficiency with fewer dedicated people. Still, more than half (52%) of respondents have no more than two dedicated employees. Many variables will contribute to the size of a third-party risk management team. Although two (or fewer) dedicated employees may seem too few, this number is still encouraging, as the number of organizations without dedicated staff has declined significantly. Only 13% reported having no dedicated employees this year, down from 24% a year ago.

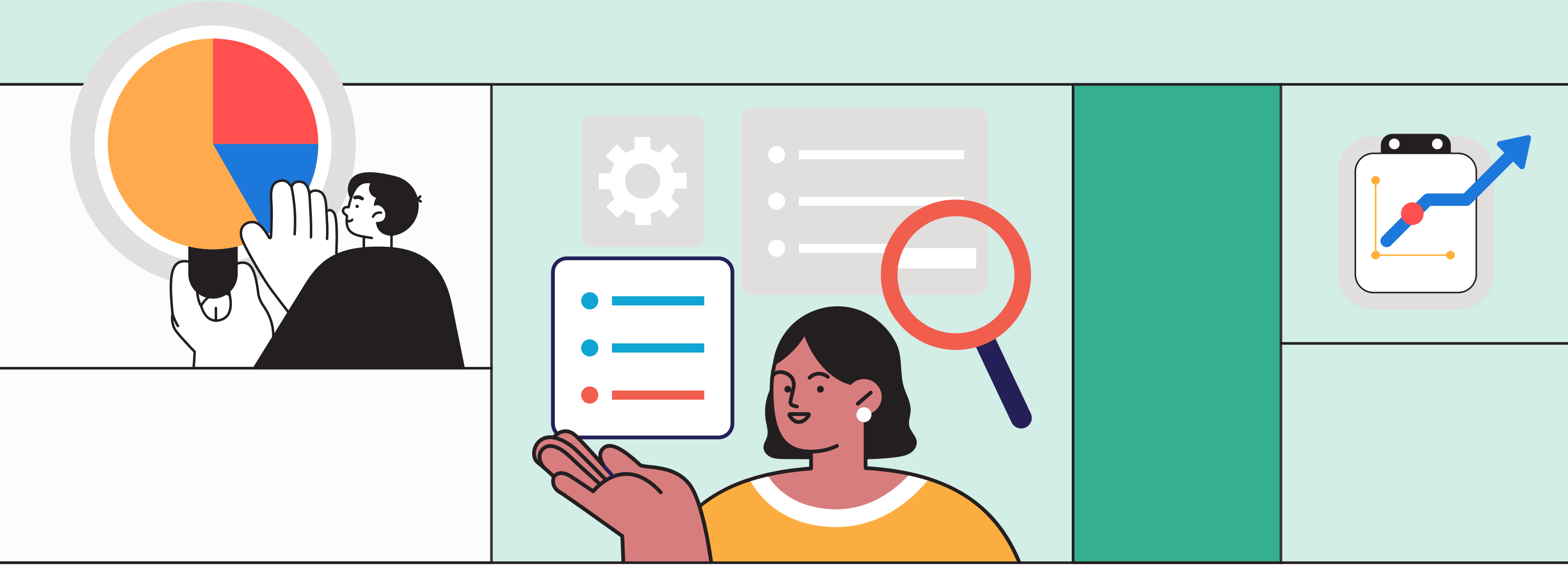
For organizations reporting more than two staff members, another 19% reported having 3-5 employees. For larger programs, the numbers remained consistent with the previous survey; 6% reported 6-10 employees, 2% between 11-20 employees, and 8% had more than 20.

Although there is no magic number when it comes to third-party risk management staffing, each organization should have enough people to accomplish the program efficiently and effectively. Third-party risk management programs can often accomplish "more with less" thanks to technology, automation, and skilled staff. Still, even the most proficient practitioner can only do so much in a day.

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

How many full-time employees are dedicated to your third-party risk management program?





Organizational Structure

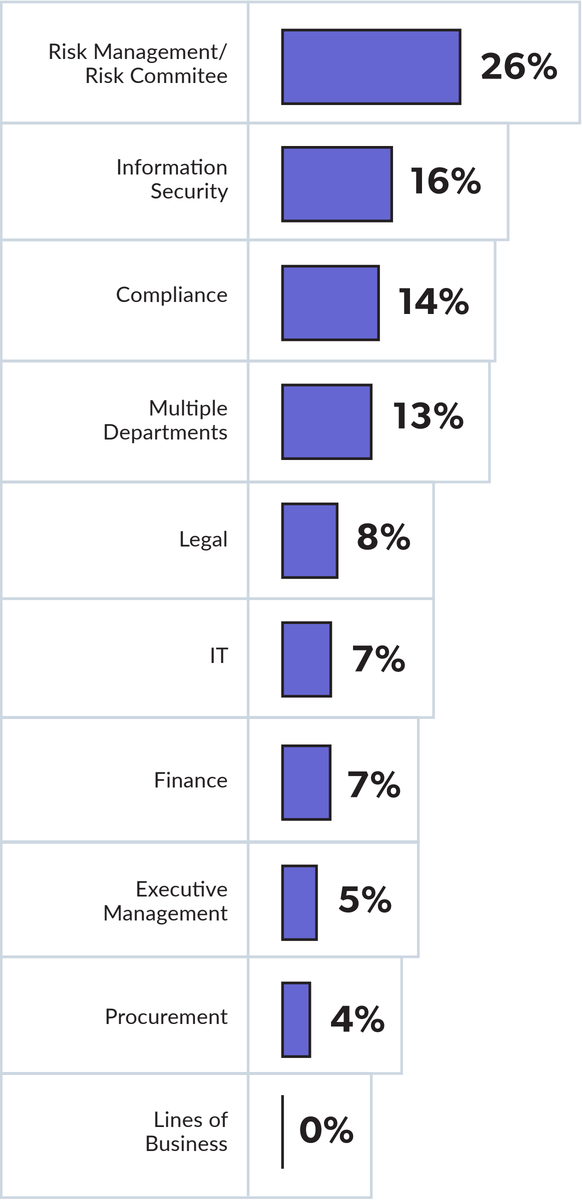
Third-party risk management programs are most successful when aligned to reporting structures that enhance and support their function as a true risk management discipline. Forty percent (40%) of our responding organizations agree and have aligned third-party risk management under Risk or Compliance departments. Another 23% of respondents report to Information Security/IT departments. Fewer organizations report to Finance (7%), Procurement (4%), or Legal (8%). Finally, 13% are reporting to multiple departments.

For the first time, no respondents reported to the Lines of Business. This is great news because third-party risk management must be able to apply its rules, requirements, and processes impartially; there should not be any conflict between third-party risk management's goals and those of a business line or other departments.

Still, not all organizations are structured identically, and many organizations have demonstrated that third-party risk management can operate well in different environments. It is essential to remember that third-party risk management is, first and foremost, a risk management discipline. The alignment of third-party risk management with a risk-focused department or function, such as enterprise risk management or risk and compliance, is a best practice, but does not guarantee success.

*What matters most is that senior leadership ensures that **third-party risk management has the right level of visibility, authority, autonomy, sponsorship, and support** no matter where they sit within the organization.*

In which department does third-party risk management report?

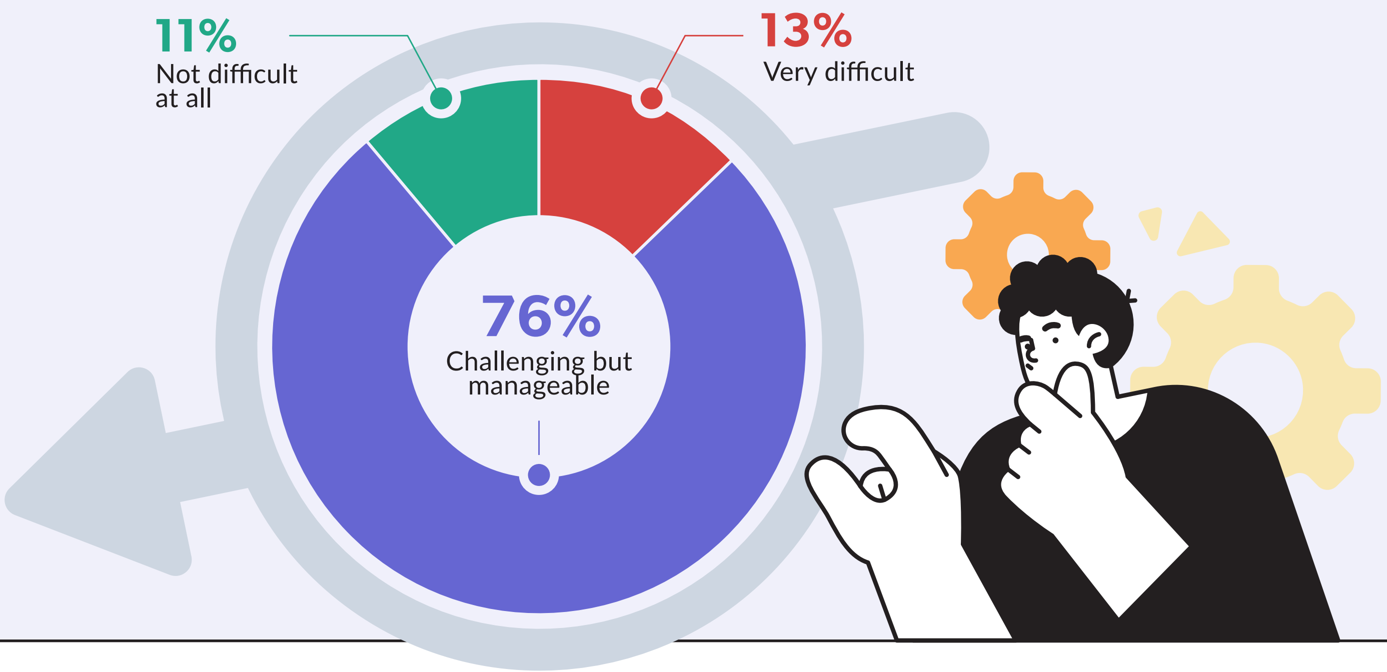


Sponsorship from the Top

It is no secret that friction with the business line or vendor owner can make third-party risk management programs less effective. Sometimes, third-party risk management activities are not prioritized by business lines or are considered secondary to the business's objectives. In other cases, business lines or vendors may push back against their assigned roles and responsibilities within the third-party risk management process. There are also many times when third-party risk management teams have to constantly chase late or missing deliverables from vendor owners. It is a painful truth that many third-party risk management teams experience these scenarios on a regular basis.

This year, 76% of our respondents found getting the line of business or vendor owner support challenging but manageable, and 13% found it very difficult. But how do these challenges reflect sponsorship from the top?

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

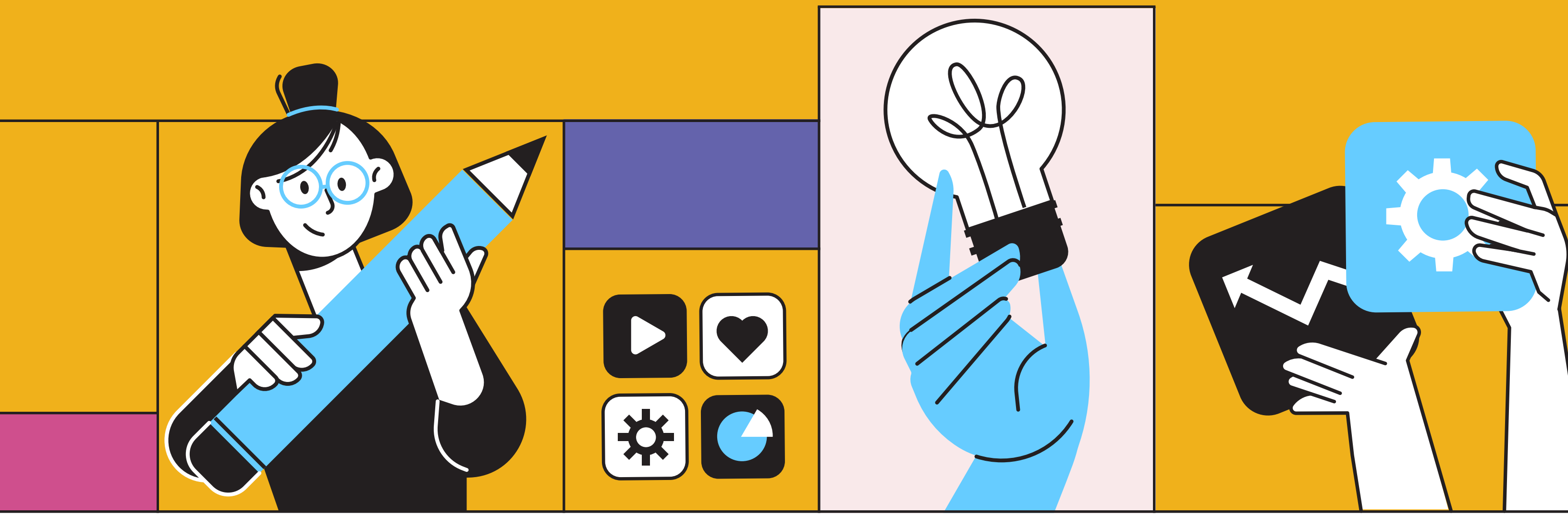


How much the business units or vendor owners support third-party risk management can often be attributed to the "tone-from-the-top." An organization's senior leadership may be unaware of its crucial role in the effectiveness of the third-party risk management program, and its actions and words have a domino effect throughout the organization. A lack of funding and insufficient resources can convey an unspoken message that third-party risk management is not a priority. In cases where business lines are not complying with third-party risk management requirements and leadership appears unconcerned, third-party risk management might be perceived as another "check-the-box" activity.

In contrast, the entire organization notices when the board and senior leadership actively incorporate third-party risk management into strategic planning and decision making. Furthermore, ensuring that third-party risk management programs are properly funded, resourced, and autonomous elevates their important role in managing risk for the organization. Additionally, senior leadership can champion third-party risk management by treating the function with the same consideration and importance as other risk functions.

Considering that only 11% of respondents had no challenges in this area, it seems that there is quite a lot of work to be done.

Organizations must ensure that leadership ***sends a strong and urgent message*** *to the business lines and vendor owners regarding the importance of third-party risk management.*



Program Investment

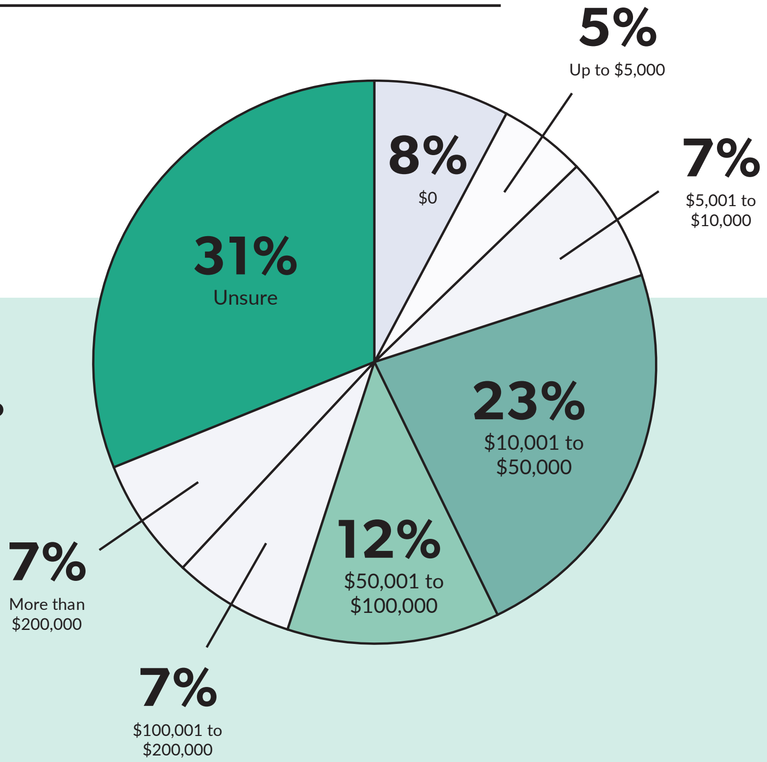
Programs must have adequate financial support. Allocating enough program dollars is essential to ensure a consistent and well-run program. At a minimum, funding should adequately support dedicated staff and third-party risk management technology. Still, other funding considerations exist, such as external expert advice, legal opinions, risk alert monitoring services, or even outsourcing portions of the third-party risk management process. Proper budgeting can help ensure a well-run and effective program. Program investments beyond staffing costs can enhance the program and optimize the time available for staff to focus on identifying and managing risks.

The survey explores program investment by examining third-party risk management program dollars (excluding the cost of personnel). Program investment is on the rise slightly, with only 20% of programs spending $0-$10,000 in 2022, compared to 26% in 2021. Twenty-three percent (23%) spent the midpoint range of $10k-50K, 12% spent $50K-$100k, and 14% cumulatively programs spent more than $100K.

It is encouraging that some investments have now been made where none existed before. Still, existing budgets have not increased significantly, and some may have declined due to the tightening economy. Even as organizations respond to the challenging economic environment, it is important to ensure that third-party risk management is not disproportionately affected by budget cuts or staff reductions.

Third-party risk management ***must remain an organizational priority*** *even when the organization is running lean.*

Besides the cost of full-time employees, how much budget has been dedicated to third-party risk management?



Third-Party Risk Management Processes

Third-Party Risk Management Processes

Size and Makeup of Vendor Landscape

When considering the size and scope of third-party risk management programs, it is important to remember that outsourcing strategies can vary greatly, and no two organizations are the same. While some organizations outsource almost everything, others may prefer to keep most activities in-house. So, the number of third parties under management is not necessarily correlated with the size of an organization.

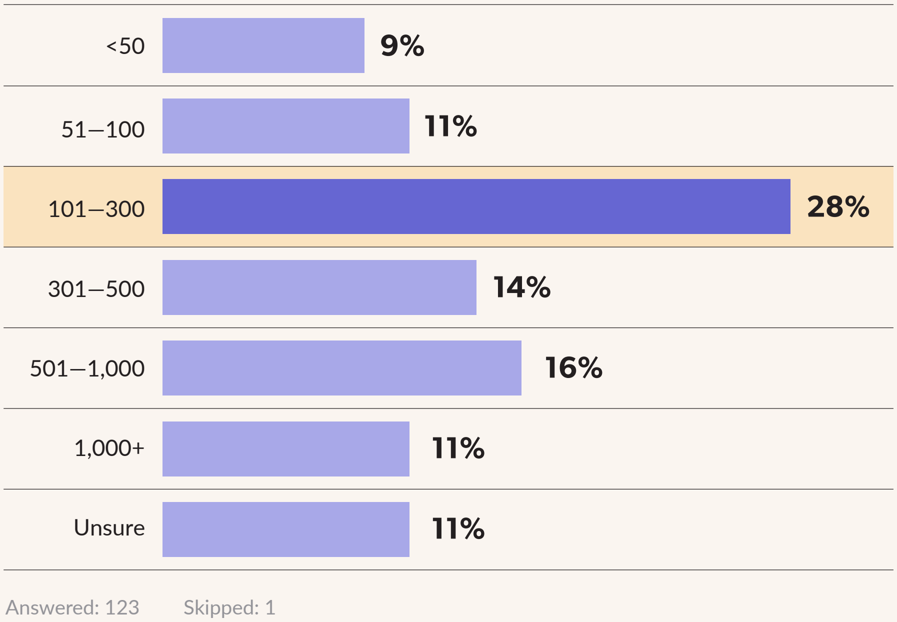
This year, our survey showed that most programs fall in the mid-size range, with 28% reporting 101-300 vendors and 14% citing 301-500 vendors. There are respondents with more extensive vendor inventories, with 16% reporting 501-1,000 vendors, and 11% stating that they have more than 1,000 vendors. Still, programs with 100 or fewer vendors represent 20% of our survey population.

Eleven percent (11%) of our respondents are unsure how many vendors they have in their programs, which can be a barrier to effectively identify and manage third-party risk. It is important to know the number of vendors and the risks they bring to your organization or customers.

What can the number of vendors in your inventory tell you?

First, it is helpful to understand the amount of risk in your vendor inventory to estimate how much effort is necessary to manage those risks. Second, the list size can indicate the effectiveness of your third-party risk management and procurement processes. Imagine that your organization is small but has a large vendor list. It is possible that some of the vendors on the list no longer have active contracts with you or still bill you for services and products that they do not provide. From another perspective, let's say that 10% of the vendors on your list sell the same product or service, such as office supplies. This may indicate that your organization does not take advantage of quantity discounts or does not have an effective purchasing strategy. Conversely, what if you have a large organization and only a few vendors, but each vendor provides many services at your organization? You could face severe concentration risk.

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



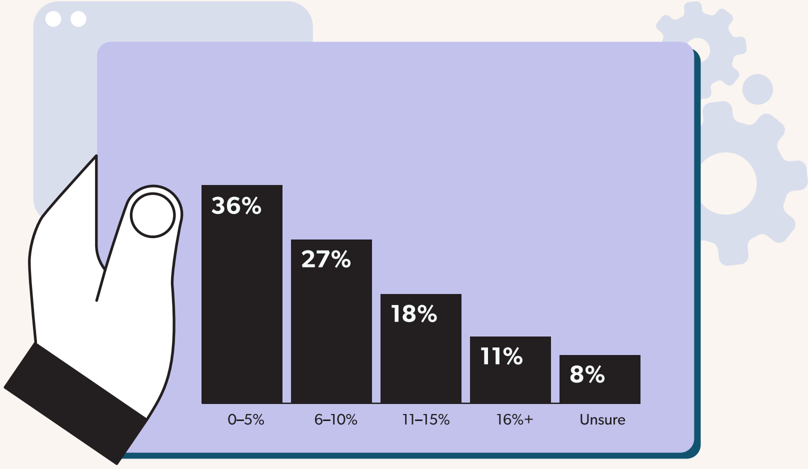
Finally, your vendor inventory can tell you if you have correctly identified your critical vendors. Suppose critical vendors account for more than 15% of your total inventory. In that case, it is time to reevaluate the criteria to identify a critical vendor or ensure the criteria have been appropriately applied.

A majority of our respondents (63%) report that critical vendors constitute 10% or less of their overall vendor population, which is in line with best practices. Despite this, 19% of respondents reported that critical vendors make up 16% (or more) of their vendor inventories. There could be a reason for those higher percentages if some organizations use critical as a risk rating rather than a business impact indicator. This issue is fairly prevalent and often results in too many vendors being categorized as critical.

The definition of “critical” can sometimes vary, but can typically be determined by these questions:

1. Would a sudden loss of this vendor cause a disruption to your organization?
2. Would that disruption impact your customers?
3. 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,” that vendor should be considered critical.



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

Operating Models

It is common for organizations to test several third-party risk management models before settling on the best one. We wanted to know how our participants approached third-party risk management and asked which of the three models they used:

EXAMPLE

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

Hybrid: Functions are shared between a dedicated team and other departments

Decentralized: Functions are managed across teams without any dedicated team

Centralized models are the most popular, with 60% reporting their use in the last year. This number is up from 48% in 2021.

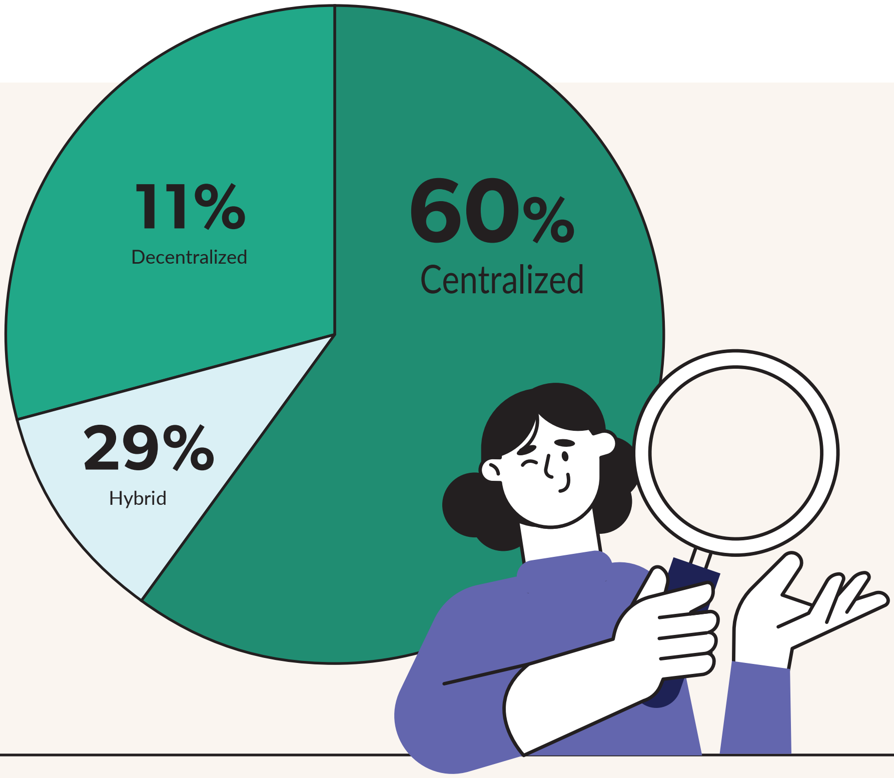
> *Since responsibility and accountability are centrally located,* ***centralized models are practical and effective.***

Those responsible for completing the tasks are familiar with the work and have experience with the processes. Despite this, there are some downsides. The vendor owner, usually in the business line, is not fully engaged in managing the risk, which results in less proactive risk identification at the business level. Vendors may also be confused about who they ultimately answer to and what should be prioritized.

It seems that **hybrid models are declining**. Only 29% of our respondents reported using a hybrid model, down from 42% in the previous year. Still, hybrid models work well and are a great option as a dedicated team maintains the program's structure and flow, keeps everyone on task, and accountable. Individual vendor owners remain responsible for vendor-level risk management activities. At the same time, subject matter experts across the organization perform vendor risk reviews. Hybrid models operate effectively when risk awareness and management are expected from everyone in the organization.

While 11% of respondents report using a decentralized model, they have some distinct disadvantages. For example, third-party risk management may not be consistent, and reporting and documentation can be incomplete or difficult to gather. In addition, additional third-party risk management tasks are not always prioritized against other business objectives and may be left undone. When organizations begin to develop their third-party risk management programs, many implement a decentralized model initially but move away from it as the need to optimize arises.

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



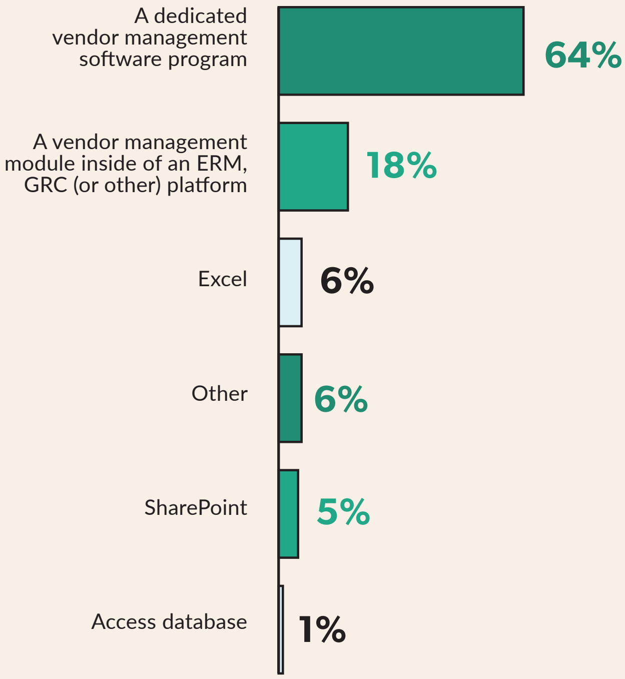
Technology Tools Used

Many processes, inputs, and outputs must be coordinated and managed in third-party risk management, many of which are strictly timebound and require meticulous record-keeping. Organizations use many different methods and tools to organize, manage, and document these activities. When asked about the primary tools used to manage vendor risk, most organizations (64%) told us they use dedicated vendor risk management/third-party risk management software or platforms.

This is an increase from 56% in the previous year. The focus on vendor risk management/third-party risk management platforms makes sense as they have been designed to address the various processes and complexities under the third-party risk management umbrella. Still, manual processes and more generic tools such as Excel, SharePoint, and Access are still used by 12% of respondents. This represents a sharp decline from the previous year's twenty-two percent (22%).

The number of organizations using vendor risk management/third-party risk management modules within another system (GRC, ERM, etc.) has remained stable at eighteen percent (18%). These solutions can be a viable alternative to manual processes and generic tools. However, it is important to remember that enterprise risk management (ERM) or governance, risk management, and compliance (GRC) applications often focus on managing an organization's overall risk and are not always equipped to manage the complex and often specialized requirements and workflows associated with third-party risk management.

What is your primary tool for managing vendor risk?



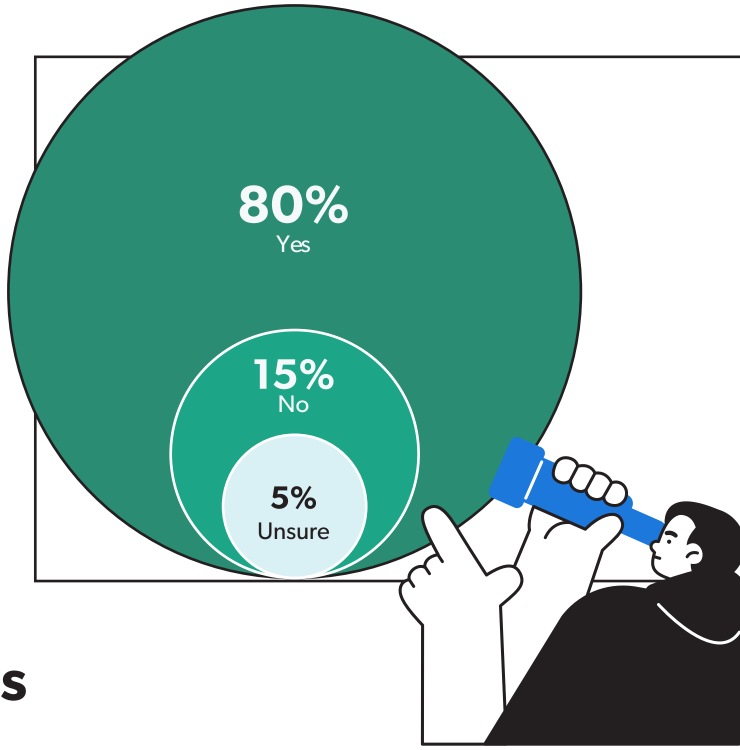
Best Practices in Third-Party Risk Management

Best Practices in Third-Party Risk Management

Vendor Criticality

Critical vendors require the most thorough due diligence, carefully drafted contracts, risk monitoring, consideration, and planning to minimize disruption if they were to fail. Auditors and regulators often focus on an organization's critical vendor relationships first. As such, it is imperative that organizations have defined criteria to identify their critical vendors. The fact that 80% of organizations surveyed have this important practice is good news. However, 15% of respondents do not currently have a process for determining whether a vendor is critical. Although that percentage is fairly low, organizations must recognize how important this process is to third-party risk management.

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

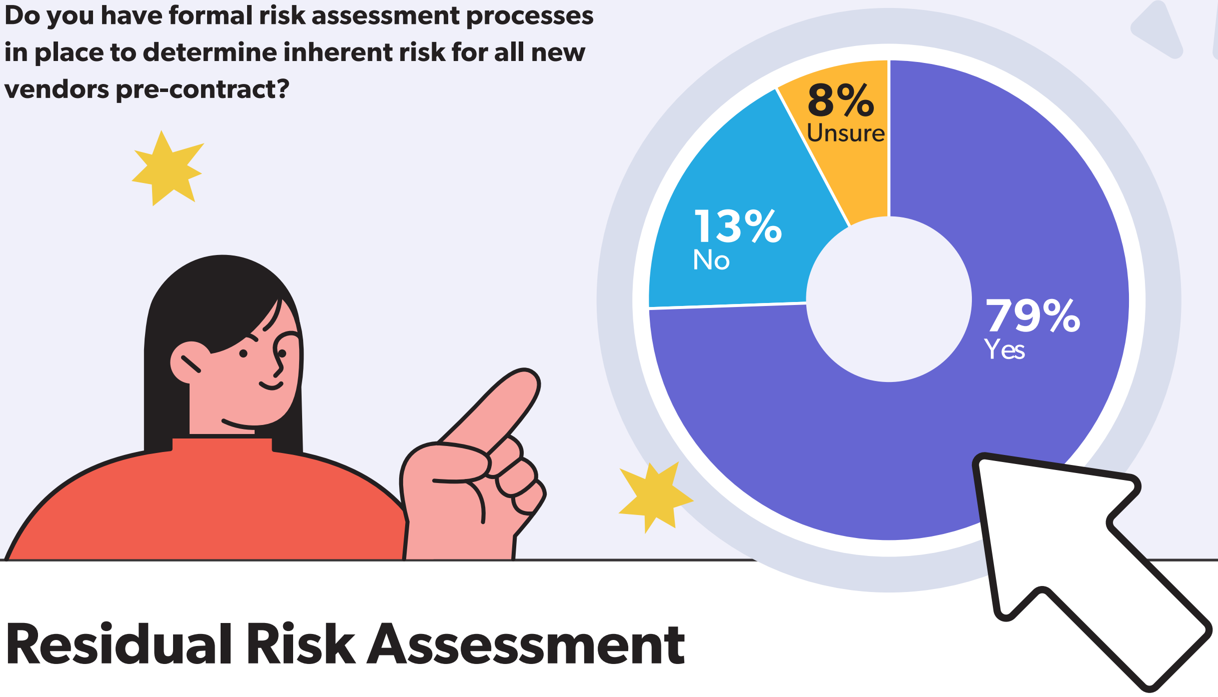


Inherent Risk Assessments

This year, we asked more specific questions about vendor risk assessments and ratings. As a starting point, we were interested in how many organizations adhere to the best practice (and regulatory requirement) of assessing the inherent risks of all vendor relationships before entering into a contract. The excellent news is that an overwhelming majority (79%) of respondents do. Third-party risk management requirements and activities are determined by inherent risk, and it is encouraging to see most organizations embracing this essential principle.

Still, 21% either did not have these practices or were unsure. The truth is that the inherent risk assessment process is fundamental to any third-party risk management program. An organization without formal inherent risk assesment processes is not only at risk of scrutiny from auditors and examiners, but they will not be able to identify and manage third-party risks effectively. Hopefully, the number of programs without inherent risk assessments will decline as newer programs mature.

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

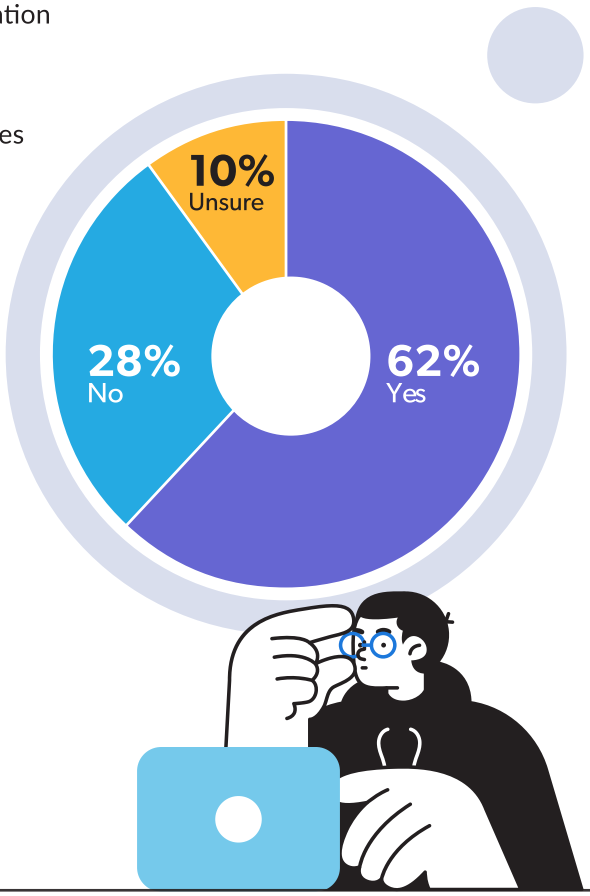


Residual Risk Assessment

Residual risk is the measure of the risk remaining after risk management practices and controls have been applied. Based on the vendor's controls and your organization's risk appetite, the measurement of residual risk can help your organization determine whether the remaining risk level is acceptable. Understanding the residual risk of each vendor engagement can also help your organization get a better view of the risk across your vendor portfolio.

Sixty-two percent (62%) of the respondents do have formal processes to determine residual risk. But 38% either do not, or are unsure. These numbers are not surprising as residual risk as a third-party risk management concept is still maturing in many industries.

*A residual risk rating **should never be used in place of the inherent risk rating**.*



Residual risk ratings reflect the confidence level in a vendor's controls. In contrast, inherent risk ratings determine the requirements for managing the vendor, including how much and what type of due diligence will be required, how often the engagement must be reassessed for risk, how the contract should be structured, and the requirements for risk and performance monitoring and management.

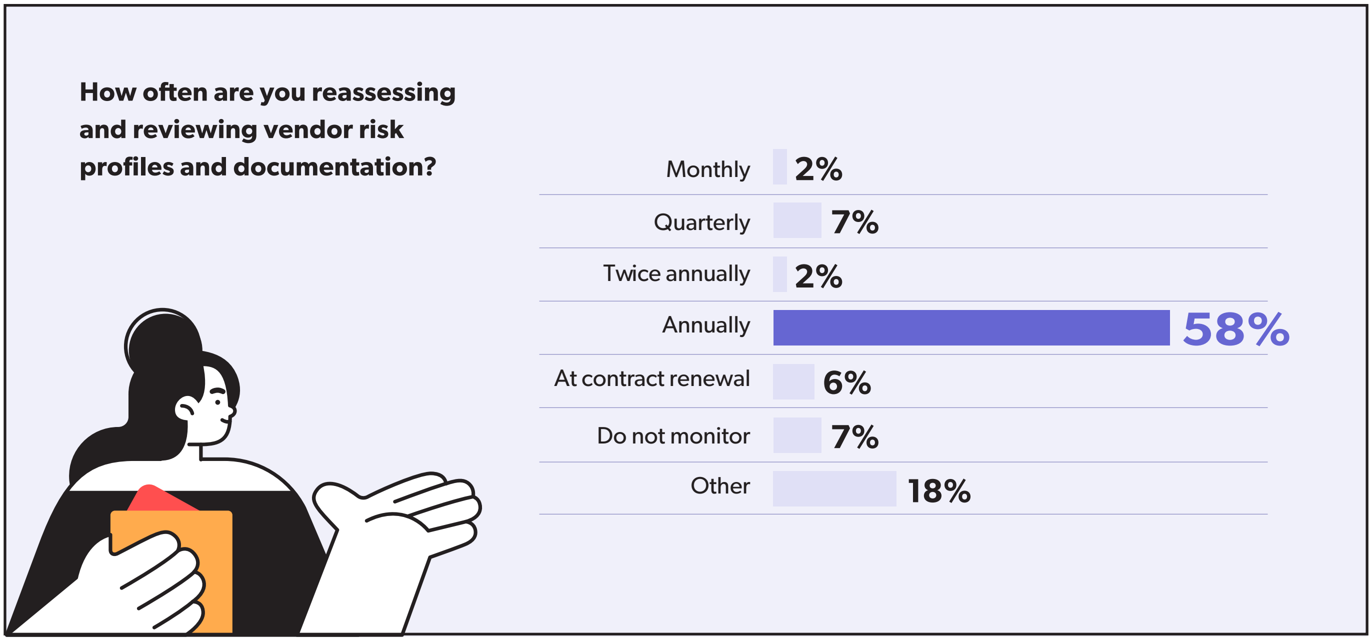
Risk Re-Assessment and Due Diligence

Periodic risk re-assessments and due diligence document collection are essential third-party risk management tasks, especially for high-risk or critical vendors.

> *As risk profiles change rapidly, waiting too long between reviews or only reviewing at contract renewal increases the likelihood that new or emerging risks will go unnoticed before it is too late.*

Risk does not follow a schedule and can arise at any time. There is no such thing as a "one-and-done" risk monitoring exercise. Still, the frequency of those "periodic" risk re-assessments or reviews should always reflect the risk and criticality of the vendor engagements.

This year, 58% of respondents said they are risk re-assessing or reviewing their vendors at least annually, which is the recommended minimum for critical and high-risk vendors. Additionally, a cumulative 11% reported an increased frequency (2% twice a year, 7% quarterly, and 2% monthly). This is consistent with findings from last year's survey. Other responses show that 18% use different frequencies. Comments provided with this question indicate that third-party risk management programs are maturing and are using a risk-based cadence to determine the appropriate intervals for risk re-assessments and due diligence document collection. However, there are still organizations (6%) that only review before contract renewal, and 7% do not perform any risk re-assessment.



How often are you reassessing and reviewing vendor risk profiles and documentation?

Current Policy

A strong third-party risk management program is based on policies that are current and follow regulatory guidance and best practices.

> *An annual policy review (and update if necessary) is a **best practice and a regulatory requirement**.*

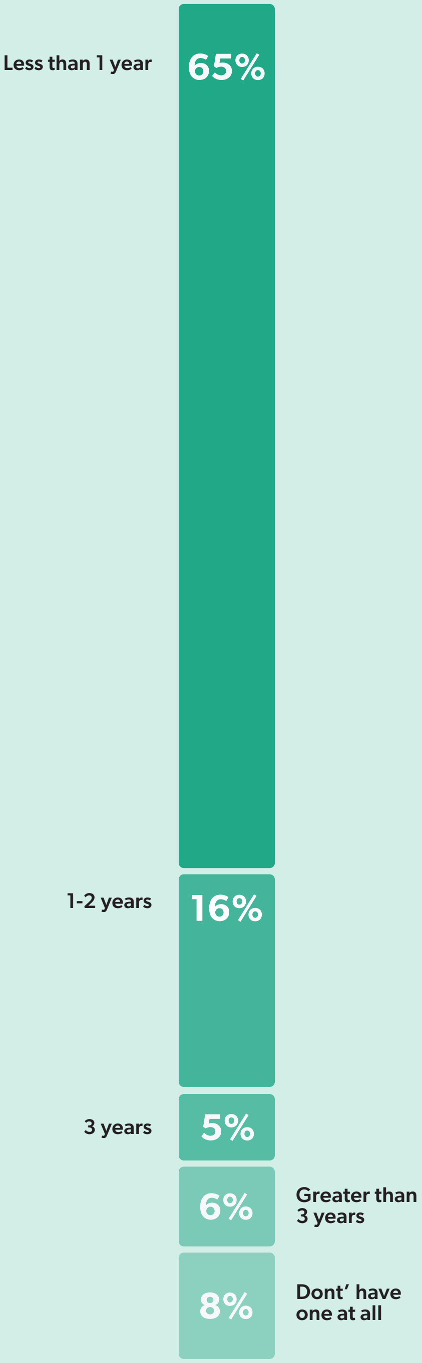
These guidelines are followed by 65% of survey respondents. That number is slightly lower than the previous year, at seventy-nine percent (79%). While 16% conduct policy reviews and updates every one to two years, another 11% report intervals of three years or more. Still, there are 8% of programs without any policy.

You should update your policy at least annually. Still, you can also update when new regulatory guidance is released, or significant changes are made to your program. It is important to know that outdated policies often result in audit or regulatory findings.

Updated Inherent Risk Assessments

In the last three years, anyone who has read the news will have noticed how exponentially third-party risks have grown since the COVID-19 pandemic. For example, risks associated with fourth parties (your vendor's vendors) are materializing in virtually every industry. So it is important to verify that your vendor has good third-party risk management practices. As risks change and new risks emerge, your inherent risk assesment must reflect the current risk environment.

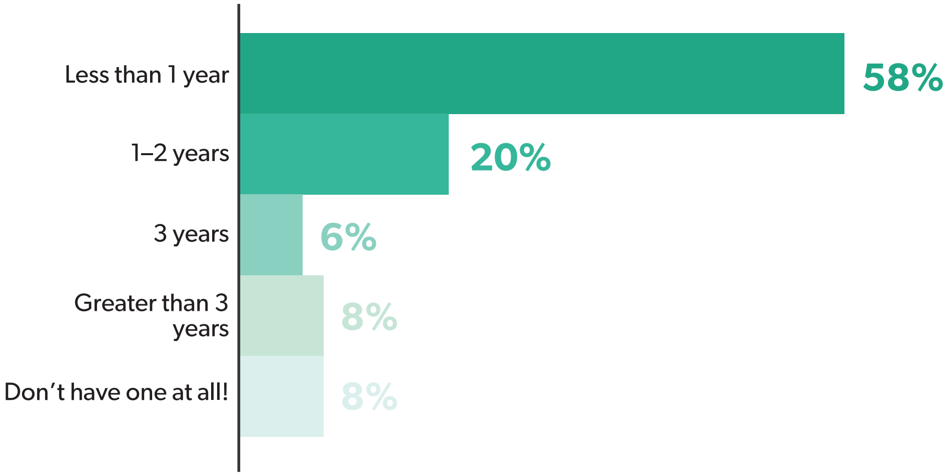
When was the last time you updated your third-party risk management policy document?

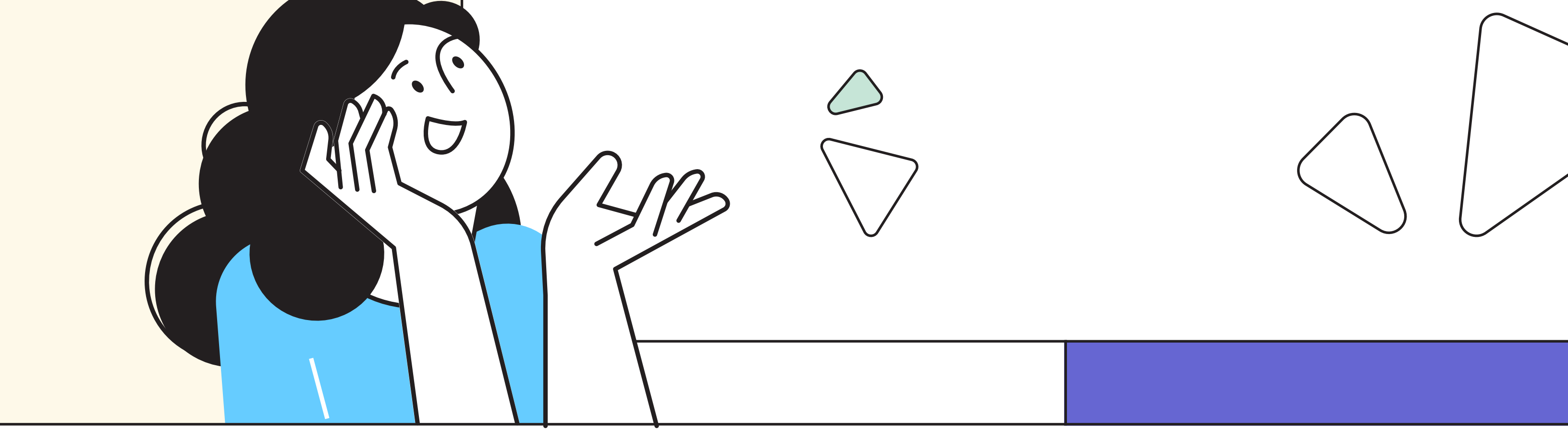


> *The quality of your risk management depends on the quality of your risk identification, and risks that are not identified are not managed.*

This means you have to keep your inherent risk assessments up to date. In our survey, 58% of respondents say they have updated their inherent risk assessments within the last year. Twenty percent (20%) have reported an update within the last 1-2 years. Those who have not updated their inherent risk assessments in the last three years (8%) or do not have any inherent risk assessments (8%) may be unprepared for emerging risks. While these numbers are consistent with the previous year, it is a best practice to review and update your inherent risk assessment at least annually.

How recently have you updated your inherent vendor risk assessment?



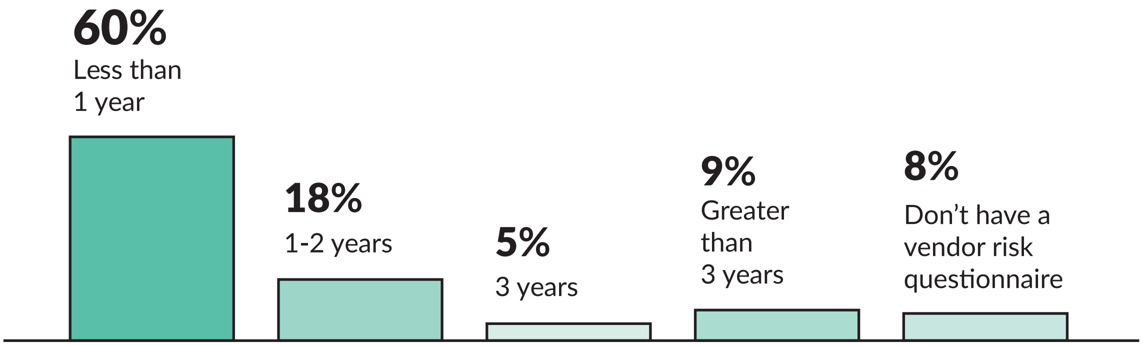


Updated Vendor Due Diligence Questionnaires and Documentation Requirements

It is important to review and update your vendor due diligence questionnaire and required due diligence documentation at least once a year. It is unlikely that vendors will proactively disclose information that has not been requested. Outdated due diligence questionnaires and document requirements will not help your organization verify and evaluate the controls necessary to mitigate new and emerging risks. Additionally, incomplete or outdated questionnaires and document requirements may send the wrong message that your program standards are too relaxed or that your organization does not take third-party risk management seriously.

It is good to see that most survey participants follow the best practice of updating due diligence questionnaires and documentation requirements annually. Sixty percent (60%) reported updates within the last year, with another 18% within 1-2 years.

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



Programs that have not updated their risk questionnaires and document requests in more than three years are overdue for an update. If you need any incentive to get started, think about how much has changed in only a few years. We are still wrestling with the long-tail effects of a pandemic; remote working is now commonplace, as are extreme labor shortages in some industries; cybercrime is now a multi-billion dollar industry; cyberattacks and data breaches are more frequent and damaging than ever; government sanctions and regulations are increasing in response to multiple geopolitical concerns; and global economies suffer from instability and high inflation. Vendor due diligence questionnaires and documentation requirements must be updated to reflect these risks (and more). As a best practice, your due diligence questionnaires and documentation requirements should be reviewed (and updated, if necessary) at least once a year or anytime there are new material risk issues or regulatory changes.

Third-Party Risk Management Growth and Pressures

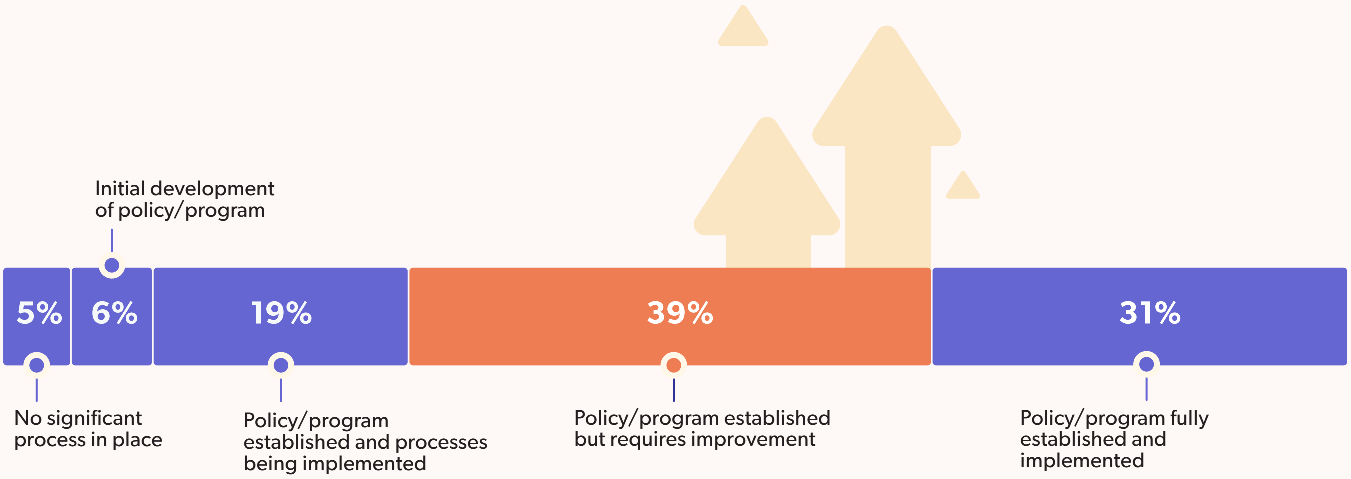
Third-Party Risk Management Growth and Pressures

Maturity of Third-Party Risk Management Programs

Third-party risk management program maturity is improving overall and even mature programs continue to improve. This year, 31% of organizations surveyed reported a fully established and implemented program, slightly up from the previous year at twenty-eight percent (28%). A further 39% respondents said that they have an existing program that needs to be improved. It is encouraging to see programs maturing, even if the pace is slow and steady.

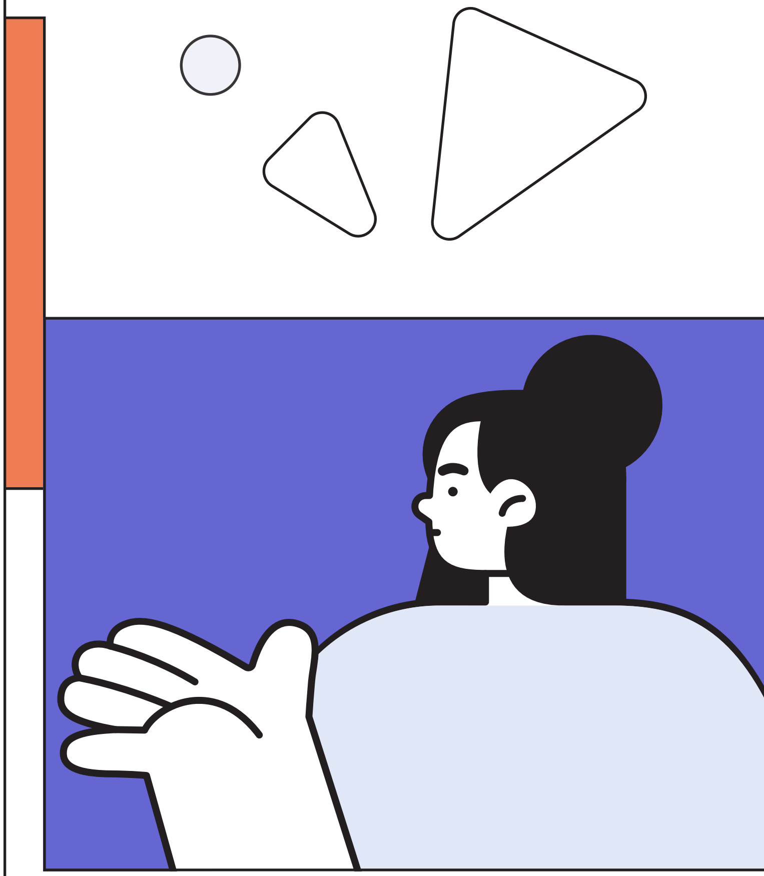
Respondents currently implementing programs account for 19%, and 6% reported being in initial stages. Finally, 5% of those surveyed said they had no significant processes in place. While that number is up from 1% last year, many practitioners and organizations are entering the third-party risk management community for the first time.

What would you estimate is the maturity level of your third-party risk management program?

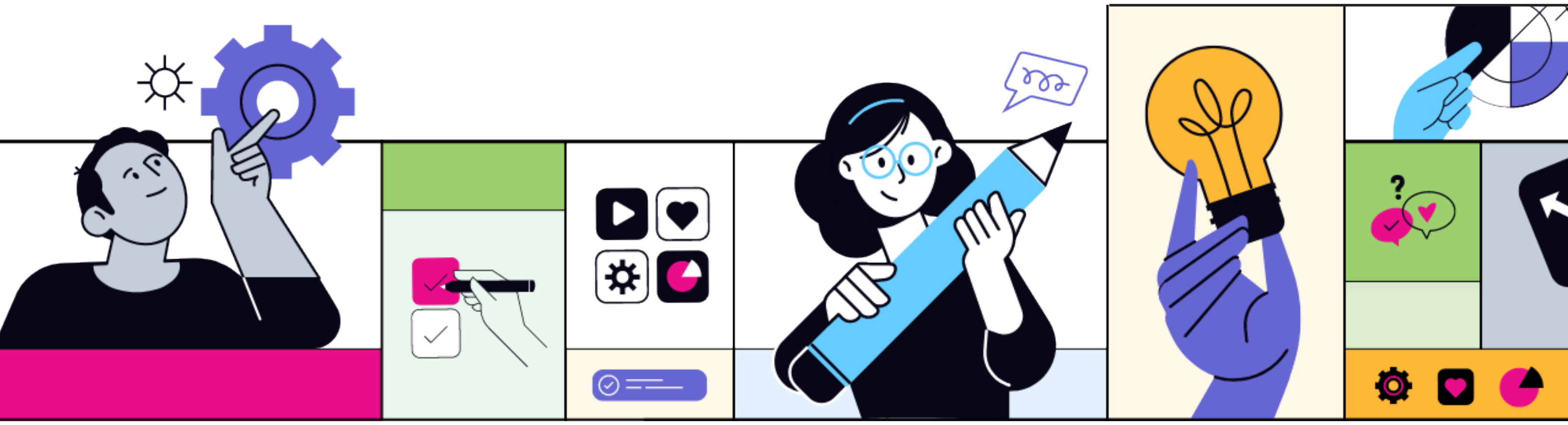


What are some signs you may need to improve your existing program?

- Core program documents are outdated, such as the policy and processes, or your procedures are hard for users to follow
- Stakeholders find your workflows confusing and difficult to use
- Audit or exam findings
- There is a low level of program compliance and a high number of late or poor quality third-party risk management deliverables
- Vendor due diligence and inherent risk questionnaires are not current enough or have poorly formulated questions that require additional explanations to internal stakeholders or vendors
- Severely backlogged work
- Only minimal reporting is available for your stakeholders



These are all good indicators that your program could use a tune-up.



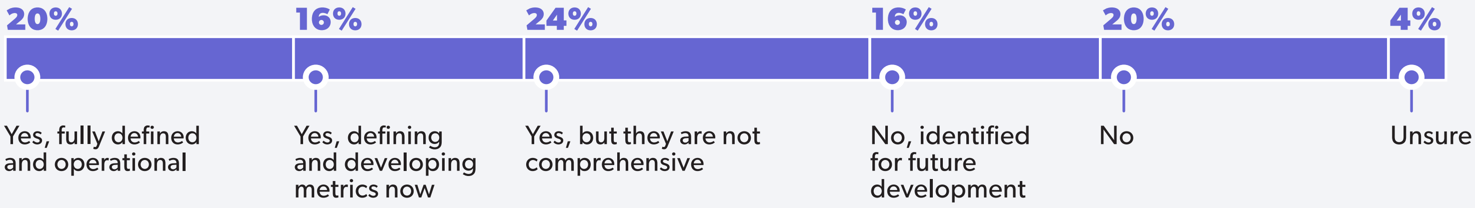
Third-Party Risk Management Program Metrics

There's a lot of interest in identifying the right metrics (KPIs) to measure the success and effectiveness of third-party risk management programs, and organizations are developing and implementing metrics and methods to demonstrate how third-party risk management adds value to their business. Third-party risk management program metrics are specific to the program as a whole and are intended to measure the effectiveness of third-party risk management programs and benchmark them against industry standards.

Understanding your program's effectiveness is essential, and confirming that third-party risk management's foundational objectives are being met is equally important. Establishing third-party risk management program metrics is the best way to holistically evaluate and measure your program's health, stability, and effectiveness.

Our survey showed that 20% of our respondents have fully defined metrics. In comparison, another 16% said they intend to develop them in the future and 20% had no program metrics at all. The remaining organizations fall somewhere in the middle. Twenty-four percent (24%) indicated that they had some metrics but they were not comprehensive, and another 16% were currently developing their metrics. While the numbers are not significantly different than the previous year's, most programs (76%) have or are developing metrics.

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



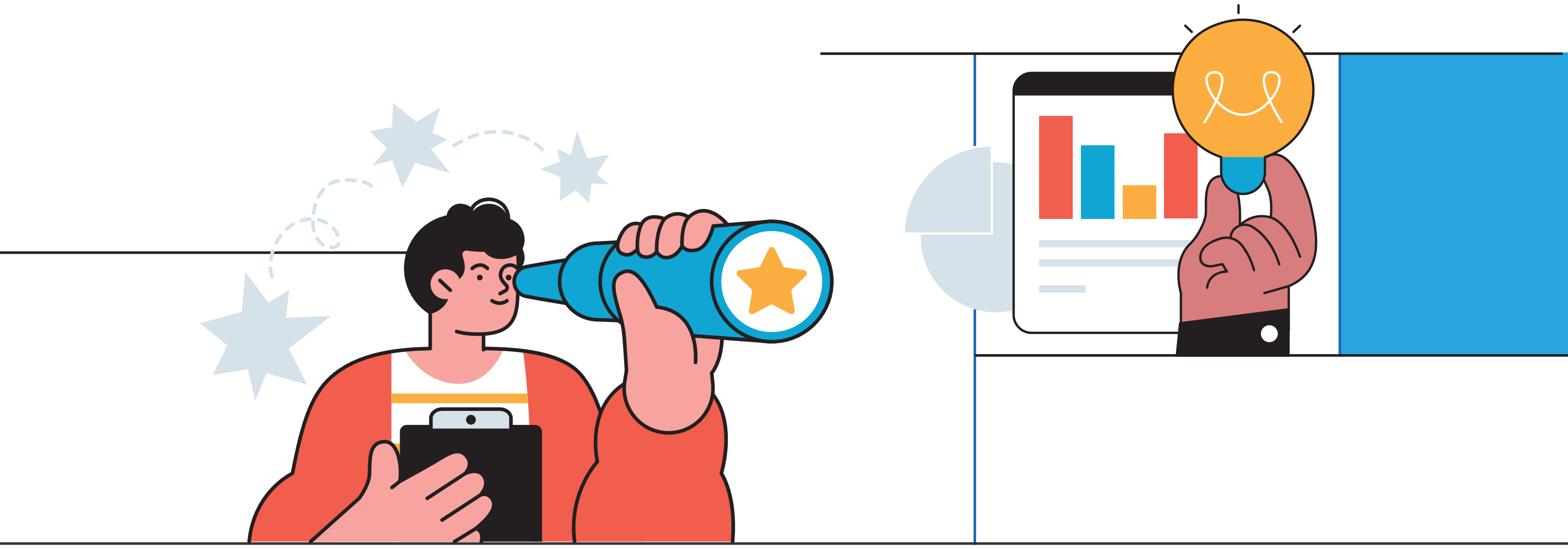
Metrics should address multiple dimensions of your program.

For example, suppose you want to show that your program is effective. In that case, you may want to measure how many due diligence issues are discovered and mitigated pre-contract or the impact of due diligence as expressed as inherent risk score vs residual risk score.

To determine program health, you may consider measuring multiple data points such as program compliance, audit or exam findings, and the percentage of high-risk and critical vendors with current risk reviews and performance monitoring.

Program stability metrics are vital and should consider your third-party risk management team capacity and the number of critical and high-risk vendors under management. Stability metrics may also include the number of vendor owners trained in third-party risk management and compliance with expected deliverables such as risk reviews and policy updates.

Developing program metrics can be time-consuming and challenging. However, once you have the methodology to measure your program, those metrics will become an integral part of the third-party risk management narrative and ongoing value statement.

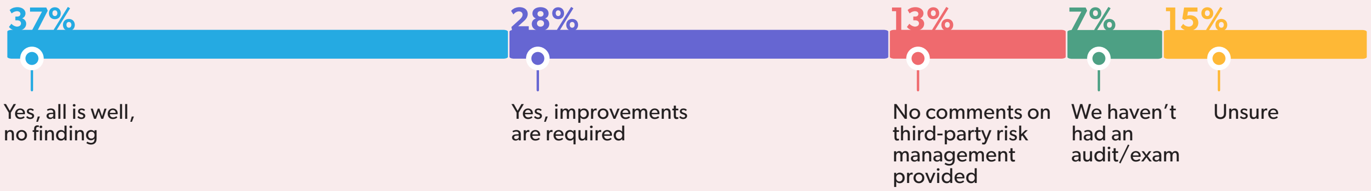


Regulatory Focus and Exams/Audit Results

More than a third (37%) of surveyed organizations had audits or exams with no findings this year. Conversely, 28% had audits and exams with findings indicating a need for improvement, and 13% reported no comments on the third-party risk management provided. The number of respondents who did not know had remained stable (15%), and 7% have not experienced an audit/exam in the past year.

Third-party risk management routines should include anticipating and preparing for audits and regulatory examinations. In addition to audits and exams, you should self-audit your program frequently.

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



As you audit your third-party risk management program, it is important to consider a few core requirements:

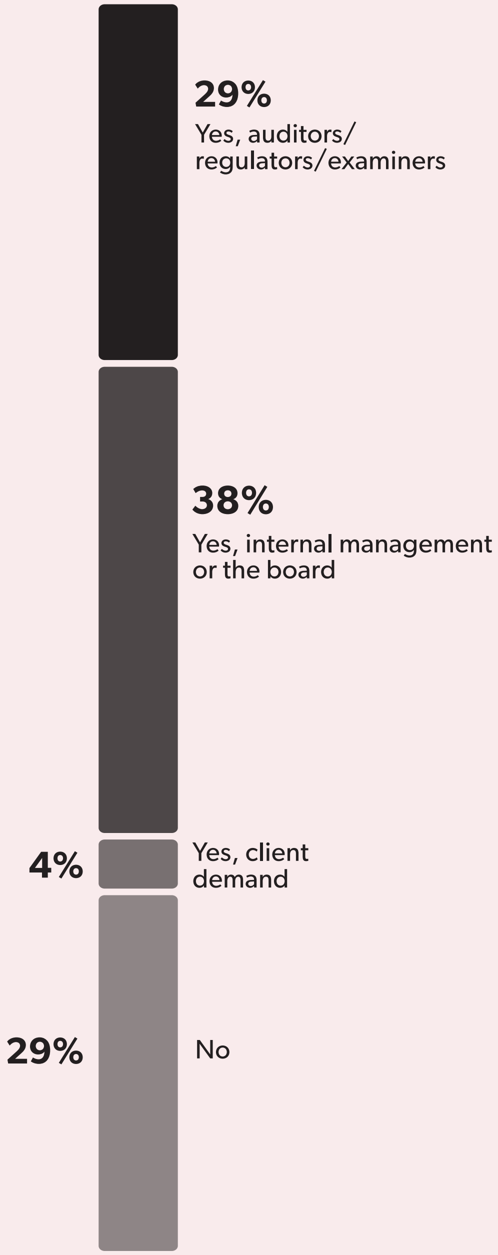
- ○ Is the policy up-to-date and in compliance with all laws, rules, and regulations?
- ○ Does your actual process align with your stated policy? If you have a requirement in the policy that is not being followed in practice, that should be a red flag.
- ○ How effective are your processes and tools for identifying, assessing, and managing risk?
- ○ Are your processes consistent? Are any exceptions documented?

The questions above are not comprehensive considerations, but can help you identify program gaps or weaknesses. Furthermore, it will allow you to improve your program before an auditor or examiner begins their assessment.

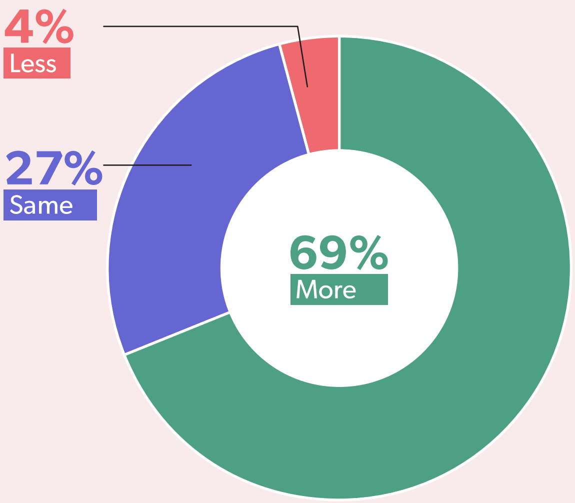
Pressures to Improve Third-Party Risk Management Programs

Interestingly, almost a third (29%) of our survey respondents said they were not feeling any pressure to improve their program, which is surprising since a cumulative 67% said they were feeling pressure from auditors and regulators (29%) or internally from the board or senior management (38%). According to 4% of respondents, customers also demand better third-party risk management. In reality, there is nothing new to report here. As regulations evolve, vendor risks expand and customer data security becomes increasingly important – third-party risk management is under increasing pressure from all sides. The best and most effective programs practice proactive, continuous improvement as a best practice vs responding to pressure.

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



From your perspective, has third-party risk management been getting more scrutiny or less scrutiny over the last 12 months by your regulators/auditors?



Regulatory Scrutiny

2022 was not overly active from a regulatory perspective, yet 69% reported feeling increased regulatory scrutiny. Though there have been few new or changed regulations, three of the largest and most influential regulatory bodies (OCC, FRB, FDIC) have proposed new interagency guidelines for managing third-party risks in 2021. As we publish this survey report, the third-party risk management community is still anticipating the final guidance.

Even though 2022 was a relatively slow year for third-party risk management regulations, a few notable changes, like the expansion of the SEC's Safeguards Rule, have kept many organizations busy. The Safeguards Rule requires "covered financial institutions," such as car dealerships and mortgage companies, to implement cybersecurity programs that incorporate third-party risk management for the first time.

New and Emerging Vendor Risk

New and Emerging Vendor Risk

Emerging Concerns

Many organizations are still experiencing the onslaught of new and emerging risks generated or exacerbated by the pandemic and all that has followed since. We asked which new or emerging threats were causing the most concern.

Here is what we learned:

70% **of survey respondents rated cybersecurity as a top concern.**

One might be surprised that this number is not higher. Examples of data breaches or cyberattacks due to third parties are everywhere. Cyberattacks and breaches hit the healthcare sector the hardest. By some estimates, those attacks have increased over 400% in the last year.

The financial services industry is also a frequent target and represents some of the largest breaches in the past few years. Still, organizations across all industries must ensure they have comprehensive processes to evaluate and monitor their vendor's cybersecurity controls and profiles.

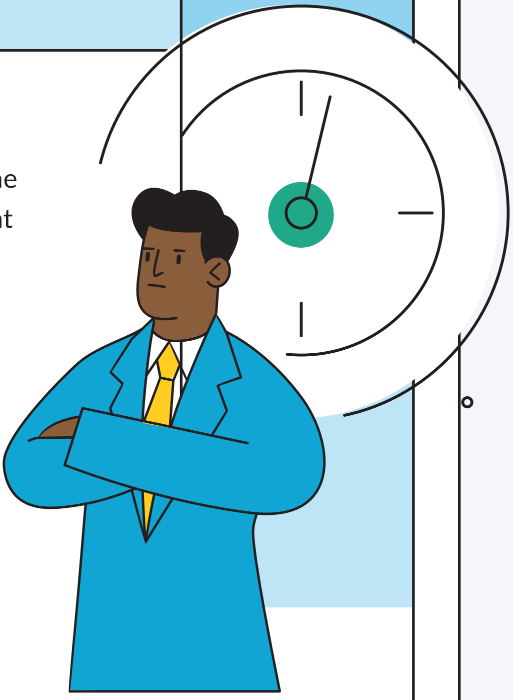
Vendor business continuity moved into the second spot at

49%

Moving up the list from number three last year, it is clear that business continuity is increasingly important. Considering the business interruptions that often result from cyberattacks and breaches, it is no surprise that organizations are increasing their focus on their vendor's business continuity and disaster recovery planning. These days, a vendor's business continuity and disaster recovery planning must consider a broad range of business interrupting events, from natural disasters, pandemics, cyberattacks, and beyond.

41%

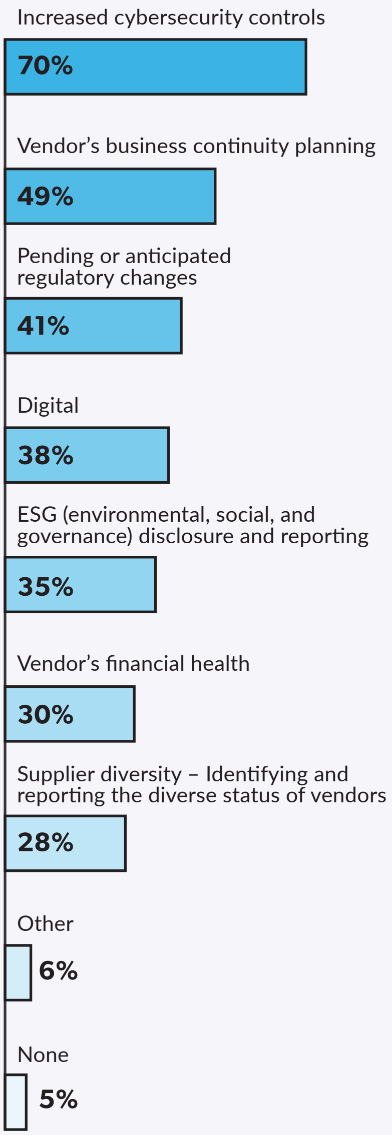
of our respondents are concerned about **pending or anticipated regulatory changes**



Regulatory changes are not a new concern but rather a “bread and butter” risk in the third-party risk management landscape. However, many organizations are awaiting pending regulatory changes, such as Interagency Guidance on Managing Risk of Third-Party Relationships, originally proposed by the Federal Reserve, the FDIC, and the OCC in July 2021. Regulatory changes can dramatically impact a third-party risk management program, from updating policy documents to adjusting workflows and processes and generating the right evidence of compliance for auditors and examiners. It is important to remember that your organization is only ever expected to comply with current regulatory requirements and guidance. Still, it is always wise to prepare for potential changes by doing a gap assessment to determine necessary changes and how your third-party risk management program can achieve them.

Other emerging concerns included digital (38%), and 35% cited ESG (environmental, social, and governance) risks. These were followed by vendor financial health (30%) and supplier diversity (28%).

Which new or emerging vendor risk areas are most relevant for your organization?



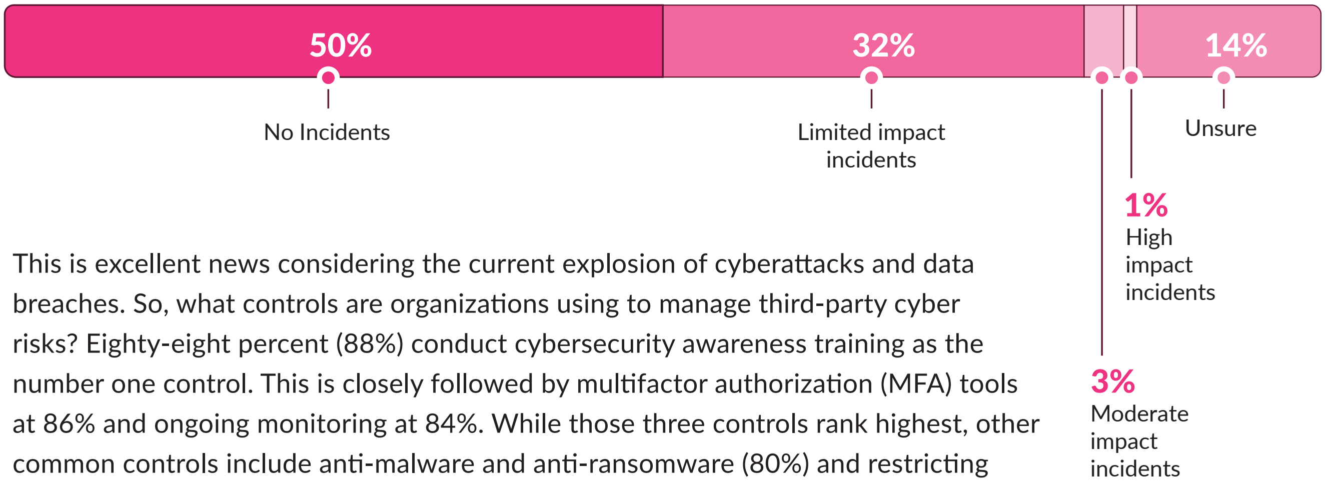
**Respondents were asked to mark all that applied*

Cybersecurity

The majority of third-party risk management programs place a high priority on cybersecurity. This year's survey included several new questions to identify how organizations address cybersecurity.

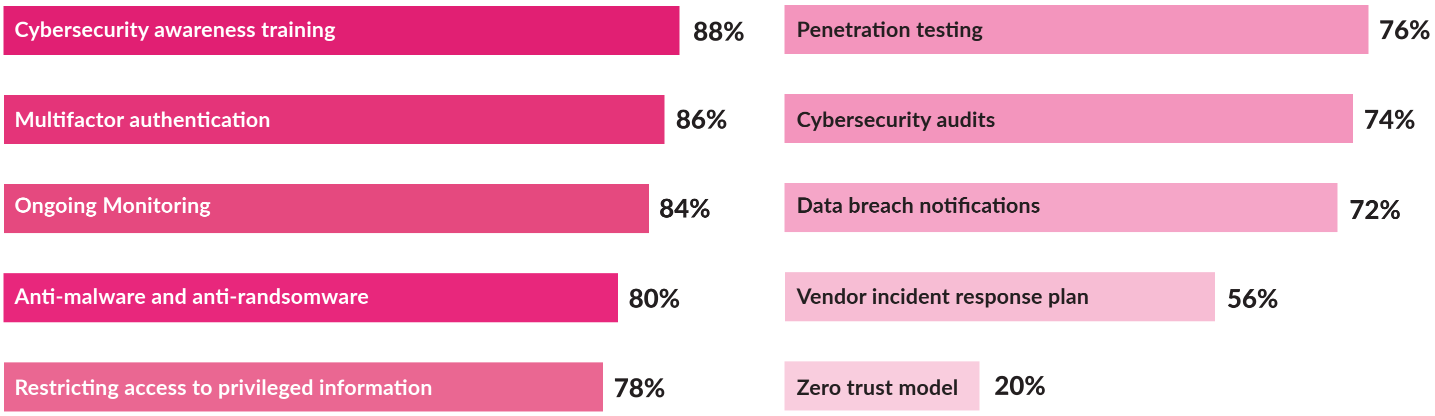
To begin, we asked how many cyber events were experienced in the last 12 months and how significant the impacts were. The good news is that half (50%) of respondents reported no cybersecurity incidents in the last year. However, more than a third of respondents reported incidents. Thirty-two percent (32%) had limited impact incidents, 3% had moderate, and only 1% suffered a high impact event in the last year.

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



This is excellent news considering the current explosion of cyberattacks and data breaches. So, what controls are organizations using to manage third-party cyber risks? Eighty-eight percent (88%) conduct cybersecurity awareness training as the number one control. This is closely followed by multifactor authorization (MFA) tools at 86% and ongoing monitoring at 84%. While those three controls rank highest, other common controls include anti-malware and anti-ransomware (80%) and restricting access to privileged information (78%). Generally, these controls appear to work well for most of the organizations we surveyed.

What controls do you use to manage your third-party cyber risks?

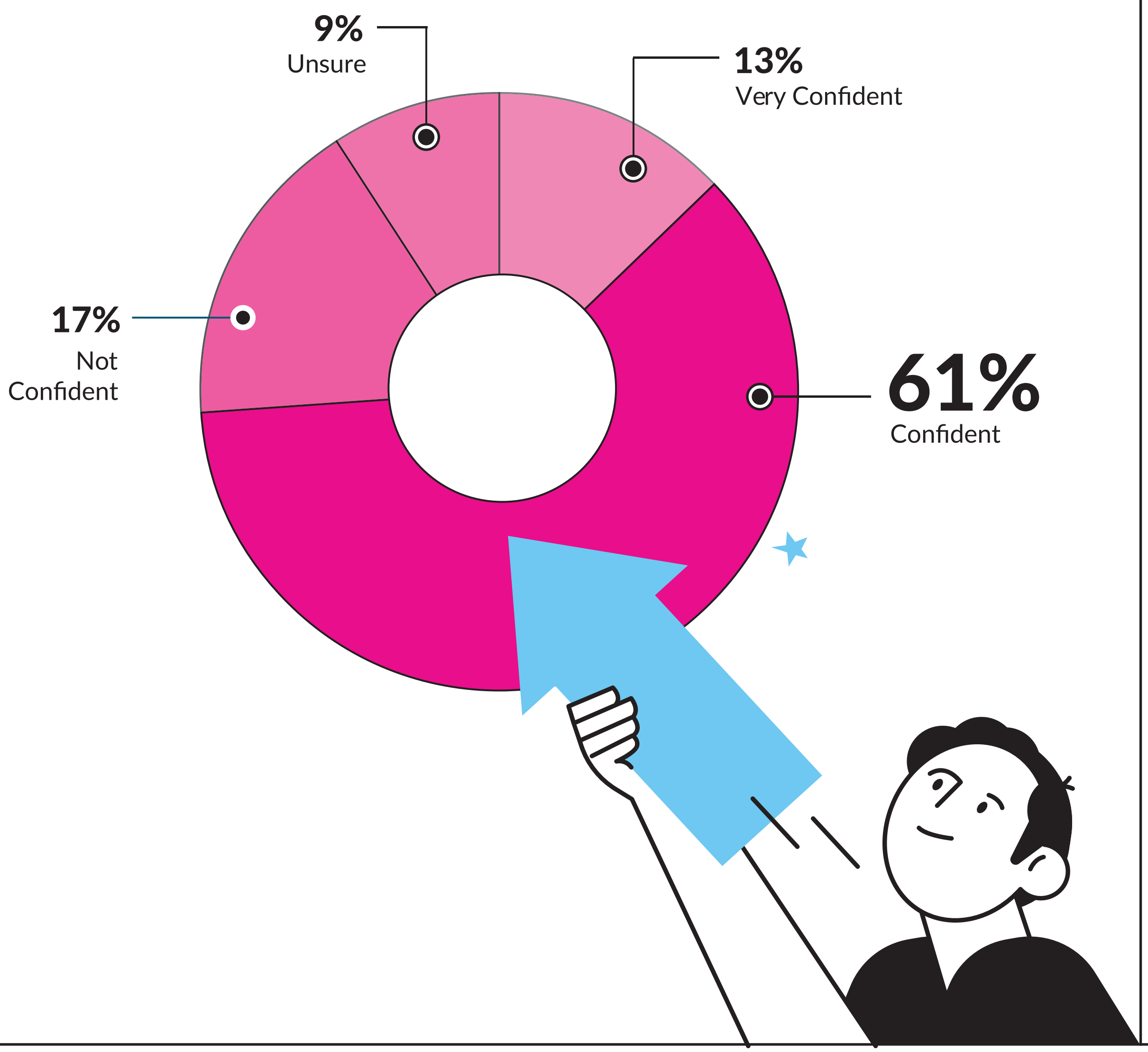


**Respondents were asked to mark all that applied*

To further consider controls, we asked our respondents to share their confidence level in the controls they use to protect their organization's sensitive information. A combined 74% reported feeling very confident (13%) or confident (61%). Still, 17% of respondents reported feeling unconfident in their controls, and 9% were unsure.

Achieving confidence in your cybersecurity controls requires constant vigilance, frequent risk assessments, and evaluation of a vendor's risk practices and controls. Keeping organizations protected and secure from cyber threats is never easy, and vendor risk is always changing. **So, organizations cannot become complacent regarding cybersecurity, no matter how confident they are in their current controls.**

How confident do you feel that all your vendors have the proper controls in place to protect your organization's sensitive information?

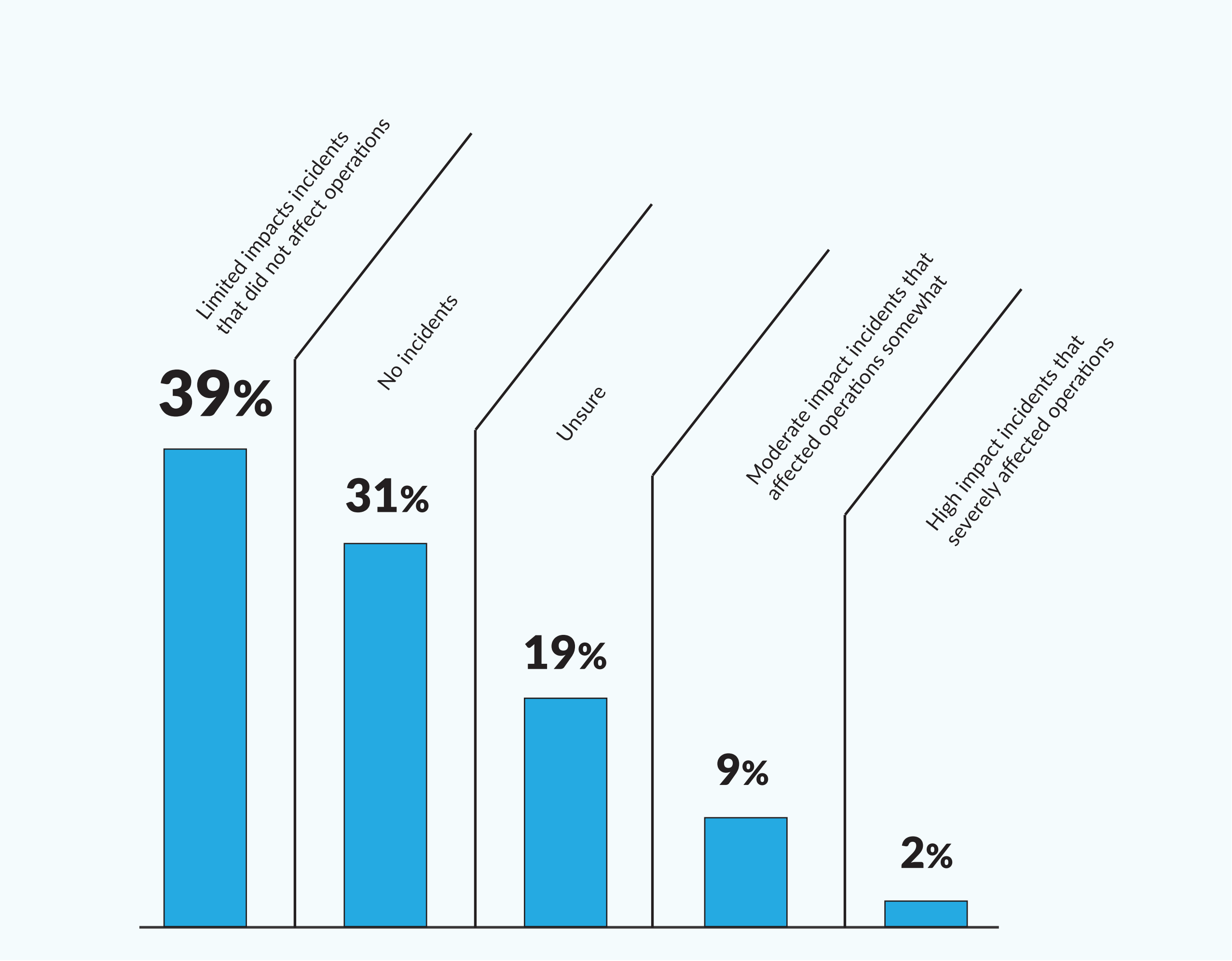


Supply Chain

As third-party risk management becomes increasingly complex, we have expanded this year's survey to include questions that consider the supply chain. The first question we asked was whether supply chain disruptions had affected the organization or its vendors in the previous year.

Thirty-one percent (31%) reported no incidents, and 19% were unsure. However, over half of those responding experienced supply chain disruption events. Of those respondents, 39% experienced incidents with a limited impact, 9% had moderate impact events, and 2% suffered from severe impact events.

Was your organization and/or your vendors affected by supply chain disruptions during 2022?

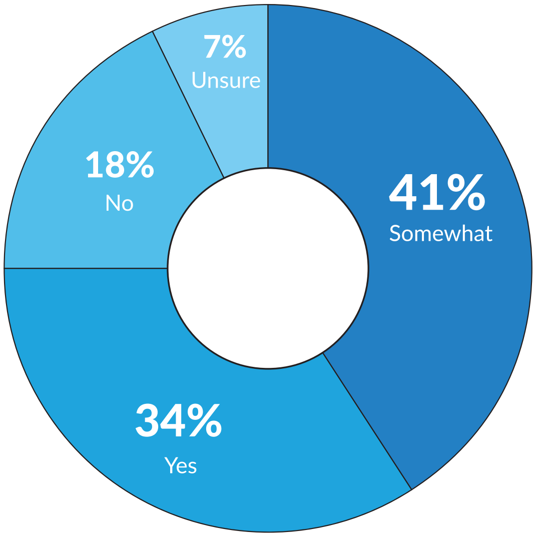


These days, third-party risk management involves more than just third parties. Fourth and nth parties are now part of the ever-expanding third-party risk landscape. So, how many organizations assess the risks associated with their vendors' third parties?

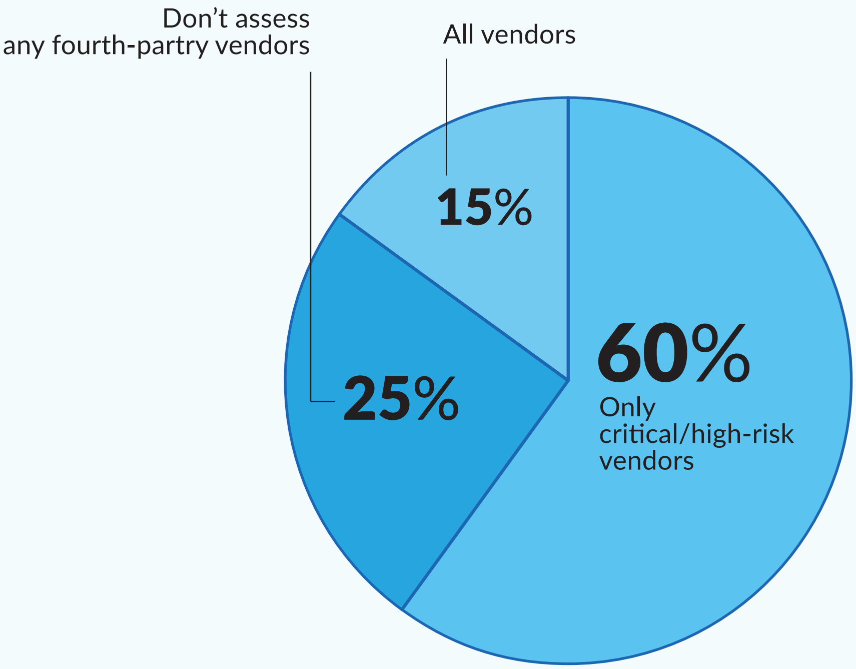
The number might be higher than expected, with a cumulative 75% (34% yes and 41% somewhat) assessing their fourth parties in some capacity. Of course, there are limits to how many extended assessments an organization can handle. This means organizations must carefully determine which extended vendor relationships to examine.

According to our survey, most organizations (60%) only consider the extended vendor risk of critical and high-risk vendors. Fifteen percent (15%) reported assessing the extended vendor risk for all vendors, and 25% do not assess extended vendor risk at all.

Does your organization assess subcontractors/ fourth-party vendors (your vendor's vendor) either directly or by reviewing your vendor's third-party risk management program?

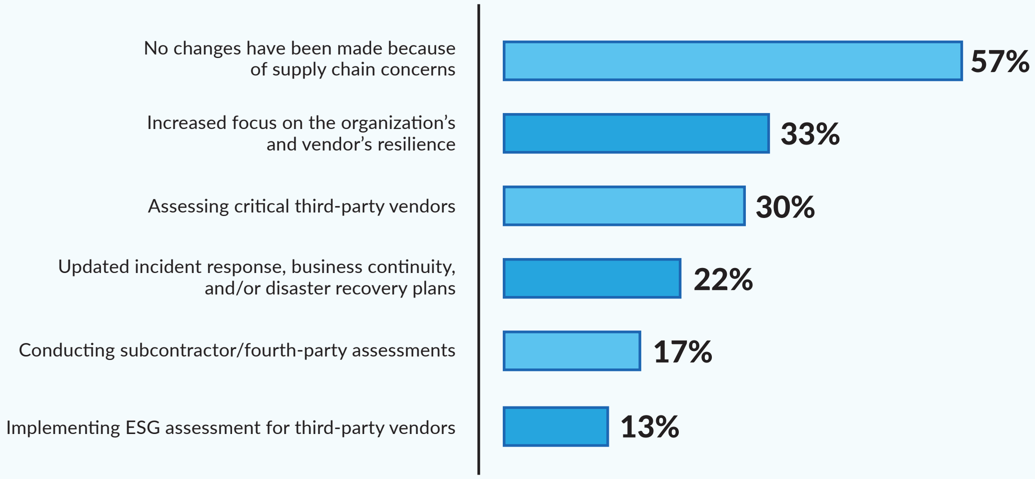


If so, for what vendors?



The survey also asked whether organizations have updated their third-party risk management activities or requirements in response to supply chain disruptions. Although 57% of respondents said no changes have been made, it is unclear whether the lack of changes reflects confidence in existing processes or if respondents are not worried about supply chain disruptions. For those who made changes, 33% increased focus on the organization's and the vendor's resilience. Another 30% assessed their vendors' critical third parties, and 22% have updated incident response, business continuity, and disaster recovery plans.

Has your organization made any updates to its third-party risk management activities or requirements in response of supply chain disruptions?



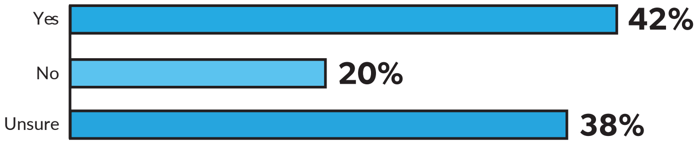
**Respondents were asked to mark all that applied*

Forty-two pecent (42%) of organizations say yes, while 20% say no. The jury's still out for the 38% who are unsure.

We often cannot determine how valuable these practices are until a major vendor failure occurs.

As they say, "hindsight is 20/20," but many organizations have begun to realize the benefits of third-party risk management, whether it helps them avoid supply chain disruptions or helps to lessen the impacts of other events such as cyberattacks and data breaches.

Do you think third-party risk management activities have helped your organization avoid supply chain disruptions during 2022?



ESG (Environmental, Social, and Governance)

On the list of rising concerns that was on page 37, ESG held steady at thirty-five percent (35%). This is in line with the increasing discussions around ESG and third-party risk management. Considering the prevalence of outsourcing, a large portion of any organization's ESG risk can be directly attributed to third-party relationships.

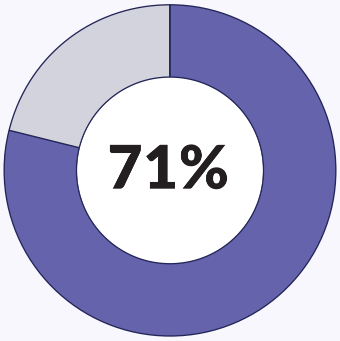
While there has been much discussion regarding ESG reporting and disclosure, in the U.S., there are few formal regulations and guidelines to follow. Of course, there are proposed regulations on the horizon (for example, the SEC's proposed Rules to Enhance and Standardize Climate-Related Disclosures for Investors). Organizations serving foreign markets like the EU and the UK will often have more experience with and a better understanding of ESG compared to most U.S.-based organizations.

Regulations aside, organizations that practice ESG transparency, disclosure, and reporting today have incentives that go beyond regulatory requirements. Consumers and investors are a significant driving force behind ESG. It could be because investors recognize that organizations that operate sustainably are more likely to survive in the long term or because consumers choose to buy products and services that align with their moral compass.

Whatever the reason, the multiple regulatory and market drivers mean formal ESG requirements are not only coming, but are here to stay.

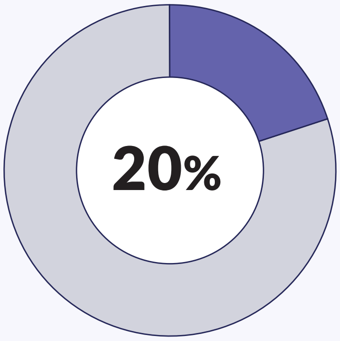
Only 9% of respondents said they were currently assessing their third parties and subcontractors for ESG compliance. Another 20% were assessing only their direct third parties for ESG, and an overwhelming majority (71%) were not performing any ESG assessments. Understandably, a large portion of those surveyed are not performing any ESG assessments at this time because there are few standards to follow. Many organizations have yet to define their organizational ESG objectives, let alone those for their third parties.

Is ESG a concern for your third-party risk management program?



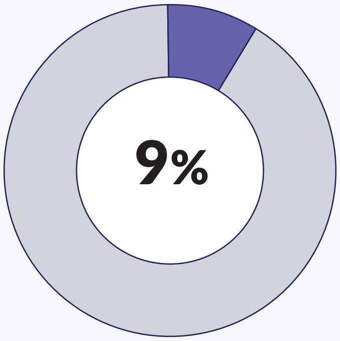
NO

We do not assess for ESG Compliance



YES

We only assess our third-party vendors for ESG compliance



YES

We assess third-party vendors and subcontractors for ESG compliance

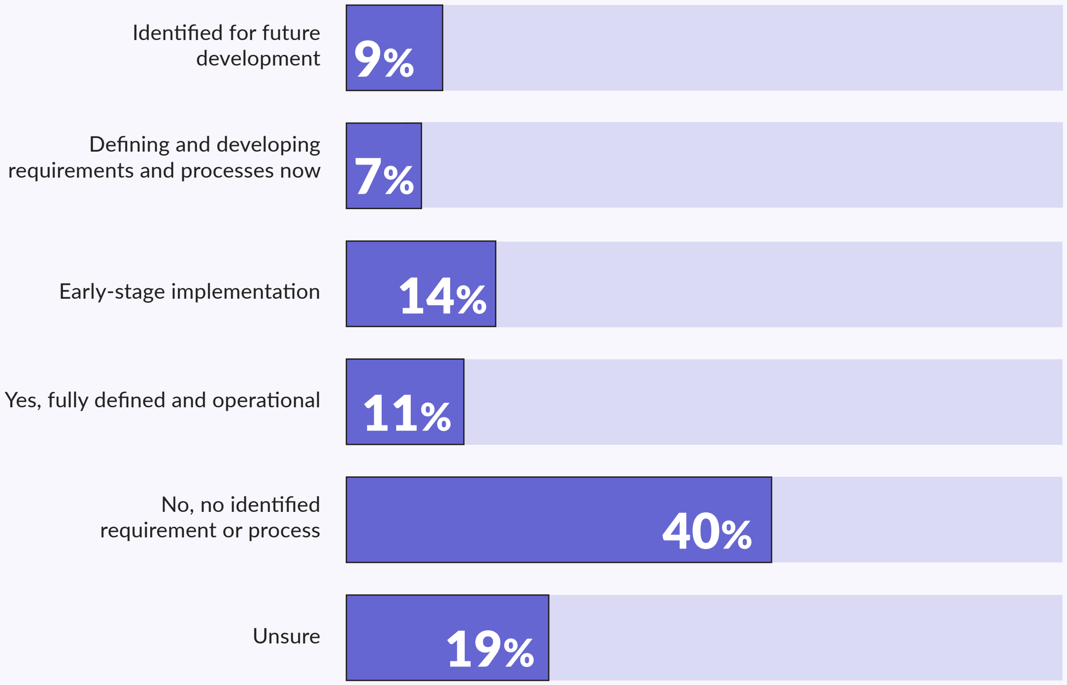
Vendor Diversity

Many financial and government institutions have specific regulatory requirements regarding vendor diversity. Other organizations include vendor diversity and inclusion as part of their corporate social responsibility programs and goals. As part of our survey, we wanted to know how many respondents included their vendors in their organizational diversity and inclusion objectives and collected vendor diversity information as part of the vendor profile.

Generally, capturing diversity as part of the vendor profile is still limited. In our survey, 40% of those responding did not capture this data as part of the vendor profile, and 19% were unsure.

But, plenty of our respondents are working towards this goal. Collectively, those organizations account for 41% of those surveyed, 9% identified it for future planning, another 7% are defining and developing the requirements and processes now, and 14% are in early-stage implementation. That leaves the 11% who have fully operational and implemented processes to collect this information.

As part of the vendor profile, do you currently collect information about your vendor's diversity status (MWDVBE)?



venminder

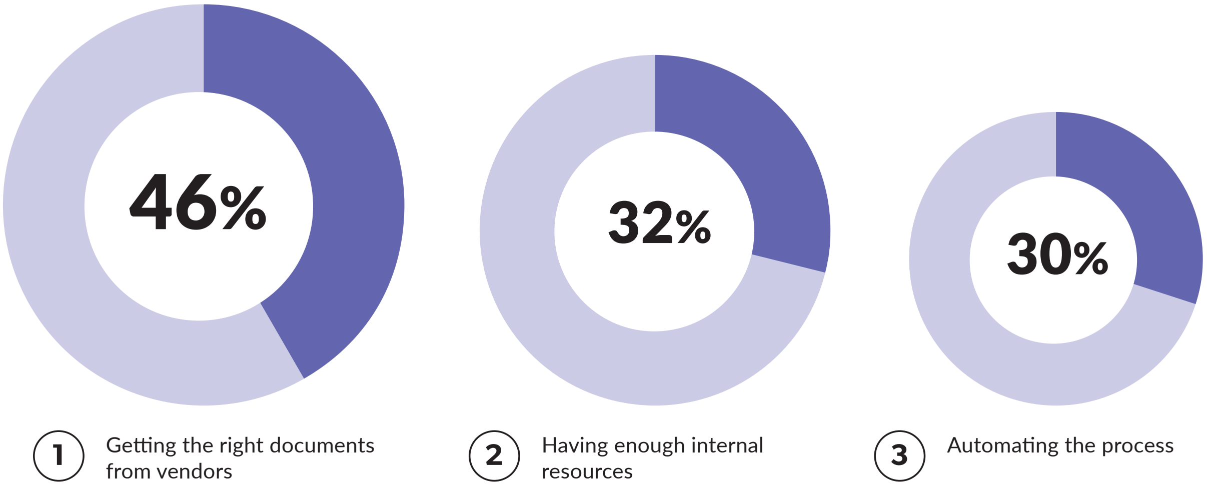
Third-Party Risk Management Challenges and Ways to Advance Your Program

Third-Party Risk Management Challenges and Ways to Advance Your Program

Third-Party Risk Management Challenges

To better understand the biggest challenges for our third-party risk management practitioners, we identified 20 areas of concern and asked survey respondents to rank their top three challenges. Predictably, the results are consistent with previous surveys.

What are your top 3 third-party risk management challenges?



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

"Getting the right documents from vendors" was ranked as the number one challenge (46%), followed by **"Having enough internal resources"** (32%). These two issues have consistently ranked as the top issues for several years in a row and were tied for first place in last year's survey. These two were closely followed by "Automating the Process" and "Time Management," which were tied for third at thirty percent (30%). It is easy to see how these challenges correlate. Certainly, gathering the right documents from vendors can be labor and time-intensive, which can eat up available third-party risk management capacity, especially if you have limited resources. Automation of processes can help improve document collection and bandwidth, but effectively automating processes is a significant undertaking in and of itself.

Unfortunately, these are ongoing challenges. Third-party risk management programs are constantly under pressure due to a lack of dedicated full-time employees and funding for third-party risk management. Time pressures are a daily reality, making the development of ways to automate the process and tailor due diligence more essential than ever.

Even in the leanest organizations, there are creative ways to address some of these challenges. A tried and true option is to utilize dedicated third-party risk management software to automate the process, improve efficiency, and keep track of documentation.

Outsourcing processes such as document collection and due diligence reviews can increase internal third-party risk management teams' bandwidth and solve document collection issues.

Training and Education

Participants in our survey were asked if vendor owners are trained to perform third-party risk management duties. The responses revealed that most organizations do train their vendor owners.

Personal instruction was a popular choice at 27%, as was providing the vendor owner with basic instructions and procedures at twenty-four percent (24%). Formalized instruction accounted for 8%, and self-service training represented 9% of the survey respondents.

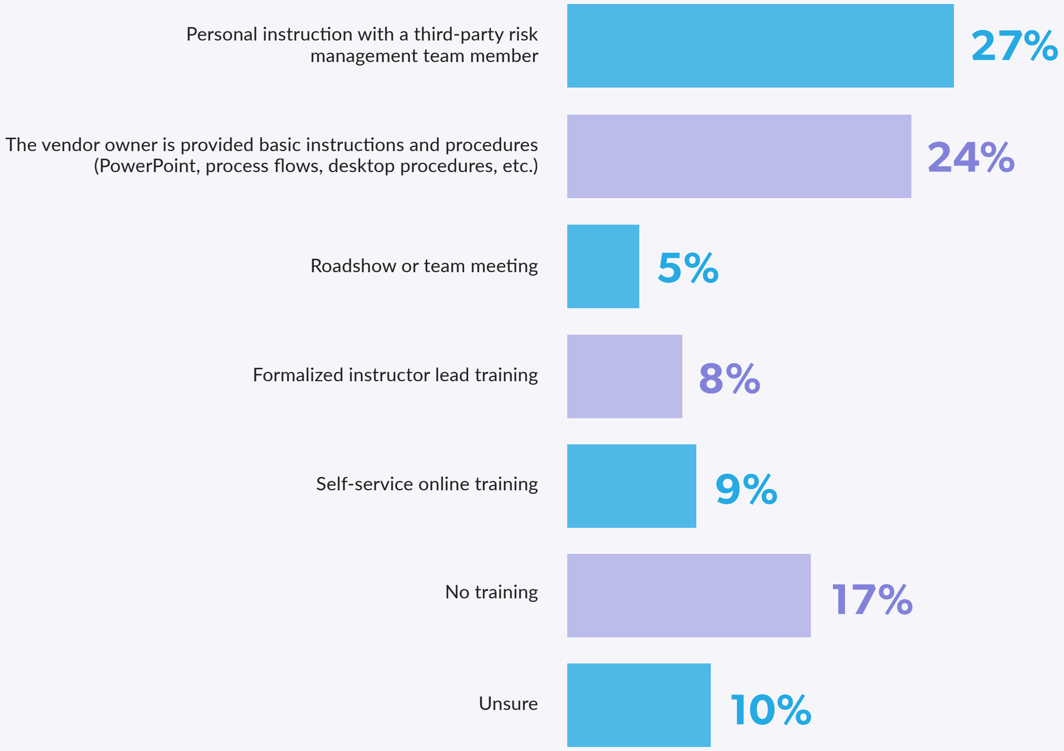
We included a question about training because it can directly influence the line of business or vendor owner support for third-party risk management. In an earlier survey question on page 11, we asked how difficult it was to secure buy-in or support from the line of business or vendor owner. For a majority of respondents, it was either challenging or very challenging.

Vendor owner training actually serves two distinct purposes. The objective is to provide practical instructions on how to accomplish various third-party risk management tasks. The second is to inform the vendor owner of the purpose and objectives of key tasks. Unfortunately, a lot of training is focused on the how vs the why. When vendor owners are instructed how to complete a task without understanding why the task is important, it becomes less meaningful and compliance suffers. This is why training is essential to create a successful third-party risk management program.

> *Good training teaches vendor owners how to complete their third-party risk management tasks whereas great training reveals the real benefits of managing vendor risks. It also creates a sense of purpose and responsibility when fulfilling the third-party risk management function.*

We encourage a review of vendor owner training materials to ensure they meet both the "how" and the "why" objectives. Training that omits the "why" is a driver for low vendor owner support and adoption.

How does your organization train vendor owners to perform their third-party risk management duties?



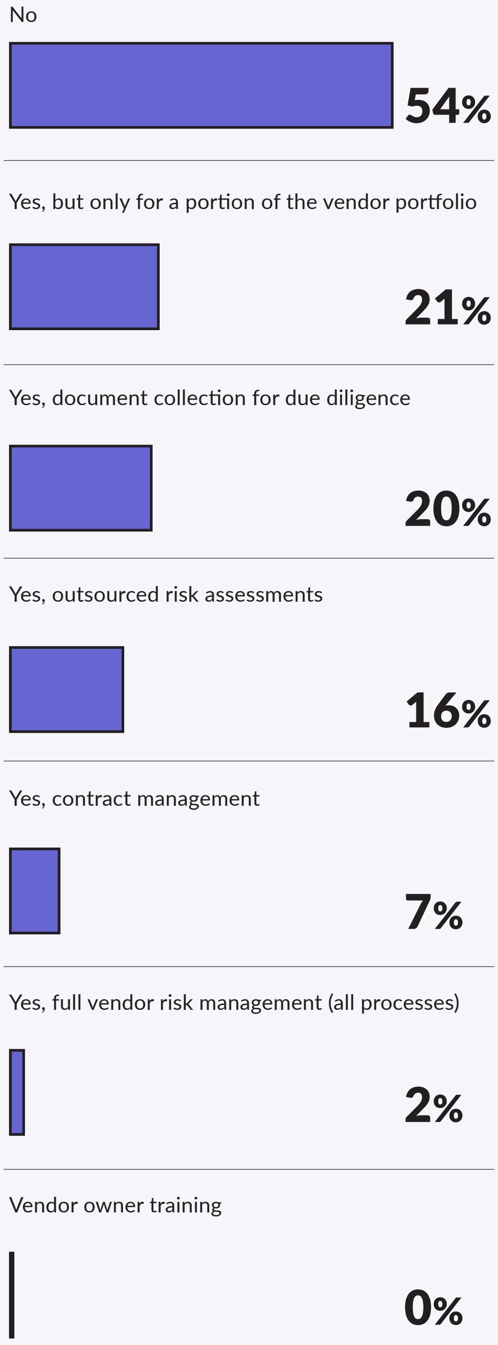
Outsourcing Third-Party Risk Management

The lack of resources is a real issue for most third-party risk management programs. **Outsourcing third-party risk management can help you accomplish more and add more bandwidth simultaneously.** You can use outsourcing for various purposes, such as conducting vendor risk reviews, collecting and organizing due diligence documentation, or supplementing your existing third-party risk management team with contractors. In this survey, we asked how many organizations were using outsourcing and what they were outsourcing.

Fifty-four percent (54%) of organizations are not outsourcing any portion of their third-party risk management program. For those who were, we found that 21% were only outsourcing a portion of the vendor portfolio while other uses include risk expert reviews (16%) and due diligence document collection (20%). A small portion (7%) were outsourcing their contract management. We predict that outsourcing will become a popular option to supplement in-house capabilities, especially as a way to solve for insufficient third-party risk management staffing.

However, we do not recommend completely outsourcing your third-party risk management program, as 2% of our respondents do. This approach may cause more problems than it can solve. Third-party risk management requires a solid internal view and understanding of the products and services provided by the vendors as well as the risks they pose. Removing internal risk management responsibilities can create a false sense of security, and emerging risks may be overlooked. While outsourcing makes sense for many organizations, be cautious about outsourcing your whole program. Auditors and examiners will hold your organization accountable for the results of your third-party risk management program, whether your choose to outsource or not. For these reasons, maintaining some internal program management is essential.

Does your organization currently outsource any portion of the third-party risk management process to an external third party?



**Respondents were asked to mark all that applied*

ROI and Primary Benefits

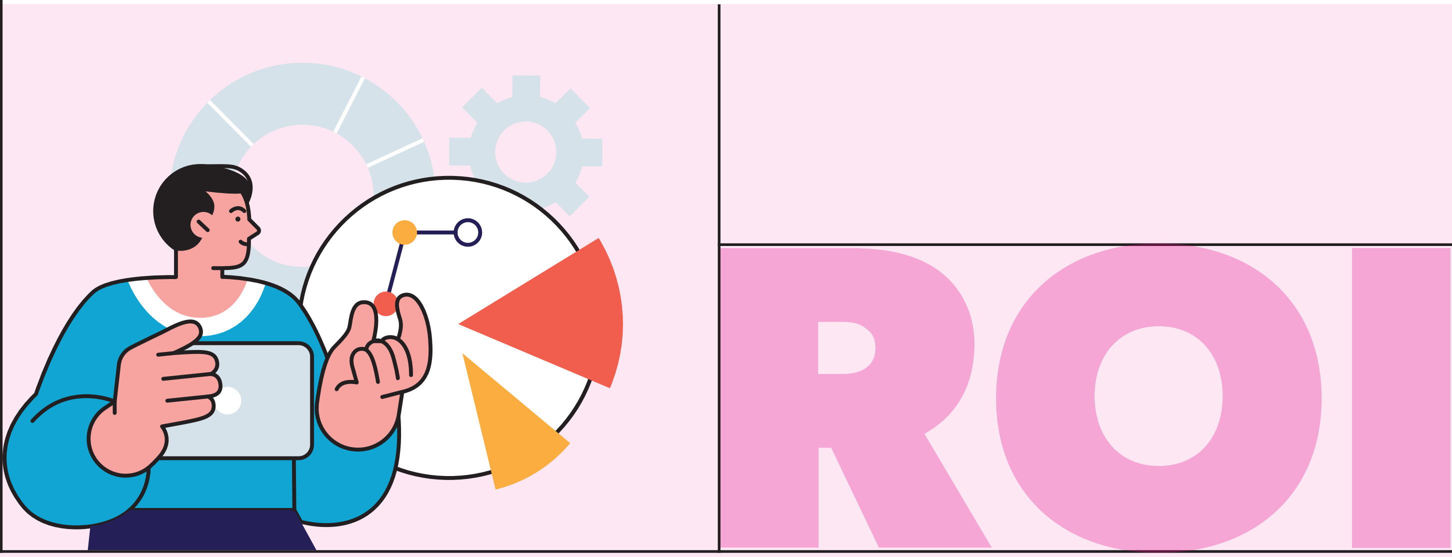
ROI and Primary Benefits

Return on Investment

How much an organization invests in a third-party risk management program is only part of a larger equation. Third-party risk management programs that deliver benefits and a return on investment (ROI) naturally enhance the commitment to the program. In our survey, the majority of respondents (68%) said third-party risk management provided an ROI. Nearly a third (32%) of organizations do not know or do not agree that third-party risk management has an ROI.

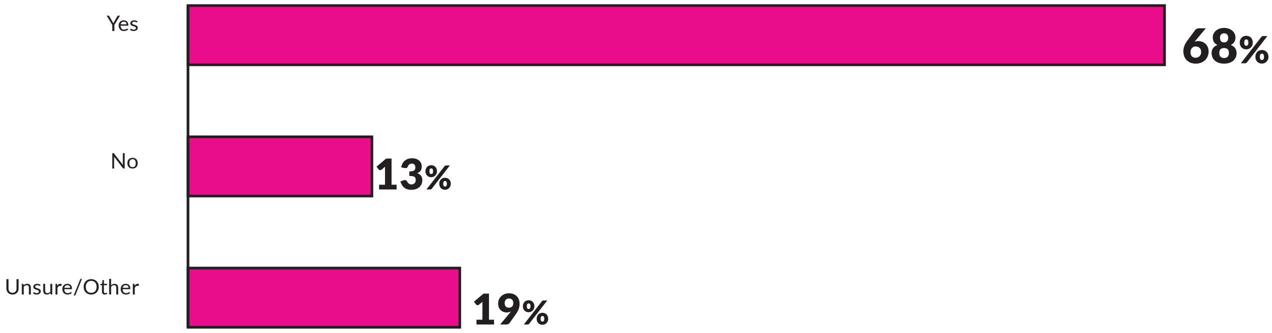
To better understand some of these numbers, it is important to consider that relatively few organizations formally measure third-party risk management ROI, so the actual benefits may not be known. It is clear, however, that many organizations continue to limit the view of third-party risk management as a "necessary evil" or "regulatory requirement." While it is true that regulatory compliance is a key driver for most programs, compliance is only one of the (some would say the most important) benefits of third-party risk management.

The benefits of proactive third-party risk identification and effective risk management extend way beyond compliance. A well-executed third-party risk management program often results in cost savings realized through improved contract management, improved third-party service levels, and proactive identification and management of vendor risk issues before they can materially impact the organization. Effective third-party risk management also reduces the likelihood of costly litigation, regulatory fines, rework, lost productivity, and negative customer perceptions.



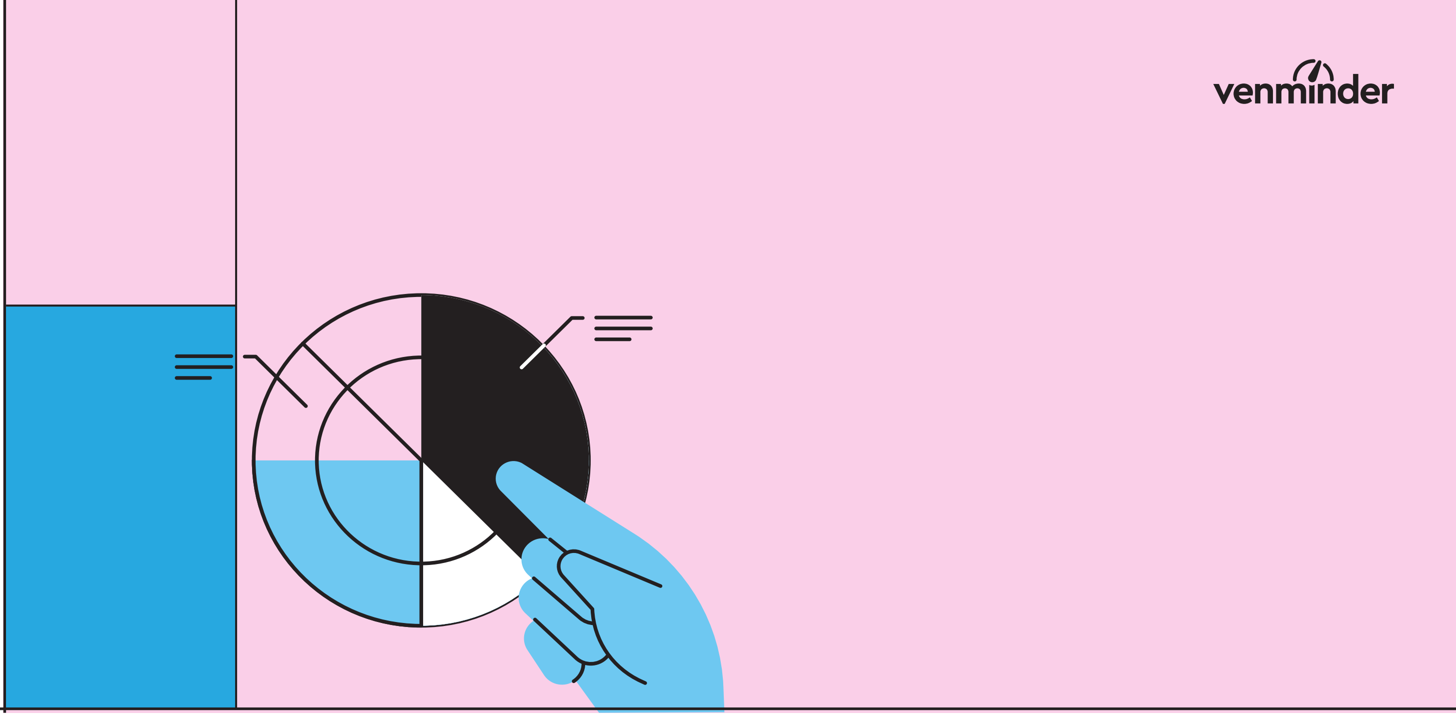
For an organization to quantify the ROI of third-party risk management, it must be able to articulate its benefits beyond compliance. Often this requires the organization to make a cultural shift away from practices that only calculate hard dollars when determining ROI. Although some benefits might be difficult to calculate into pure financial equations, it is clear what can happen if third-party risk management is not implemented or performed ineffectively. Data breaches are a perfect example. Third-party risk management is instrumental in identifying and verifying vendor information, cybersecurity process, and controls. Without these essential practices, vendor data breaches' likelihood, occurrence, severity, and impacts grow exponentially. So just how bad can it get? How much money could a breach cost your organization?

Does your organization believe there is a return on investment (ROI) from efficient third-party risk management?



Per the IBM Ponemon Institute's 2022 Cost of a Data Breach report, the cost of a data breach is averaging $4.35M. The average cost, which is at its highest-ever level, grew 2.6% from 2021 and 12.7% in 2020. Healthcare breach costs rose to $10M per breach in 2022, up 41.6% over 2020. In terms of cost per breach, financial services firms come in second at $5.97M, followed by pharmaceuticals at $5.01M, technology at $4.97M, and energy at $4.72M. These numbers show that the investments required to sufficiently staff and maintain an effective third-party risk management program are minimal compared to the cost of a breach. For every vendor that has access to an organization's (or its customer's) sensitive data, there are potential breaches.

Assume your organization has ten vendors with access to sensitive data; if just one vendor breach is avoided because of third-party risk management, that represents approximately $4.35M. Now, if you want to extend that calculation to all ten vendors, that puts you in the neighborhood of $50M worth of cost avoidance. Compare that to the cost of running your third-party risk management program – talk about excellent ROI!



Benefits

The practice of third-party risk management reduces the risk of incidents related to vendors, such as operational interruptions, reputational damage, and excessive spending. Still, regulatory compliance remains the number one reason why organizations manage vendor risk. While meeting the regulators' expectations is a primary driver, compliance does not wholly encapsulate the value of third-party risk management.

Respondents ranked their primary reasons for doing third-party risk management out of seven choices we provided. The rankings fall in line with other results of our survey.

Rank 1 to 7 your primary reasons for doing third-party risk management.

1. Regulatory requirements
2. Best practice
3. Reputation protection
4. Avoid third-party cyber incidents
5. Quality assurance
6. Cost control
7. Increased focus because of supply chain disruptions

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

We asked this year's respondents to share in their own words what they believe are the primary benefits of third-party risk management. We've highlighted the answers below, removing duplicate answers.

It is clear that there are many benefits to third-party risk management.

Compliance with regulations, awareness and tracking of third-party risk, **coordinated/centralized processes and tools**.
Bank, Greater than $10B

Protects the firm from risk.
Wealth/Asset Management, 1-100 employees

Repository for **tracking and retaining vendor information**.
Bank, $1B to $10B

Ability to proactively identify and mitigate third-party risks before they affect the business.
Technology Services or Software, 5,000+ employees

Risk minimization and **oversight on our partners.**
Real Estate/Financial Analytics, Greater than $10B

Ability to **better analyze** and see the bank's entire ERM.
Bank, Greater than $10B

We will have a handle on our third-party inventory. We will be able to risk remediate and mitigate accordingly. With the enhancement of the program, we will **see commercial benefits.**
Insurance, 5,000+ employees

Visibility into our partners and an opportunity to **focus on mission critical vendors** which could have material adverse impact on our business.
Fintech, 1,001-5,000 employees

Assurance of continuity of services, protection of information assets.
Bank, $1B to $10B

Risk management, **information security management.**
Bank, Less than $1B

Managing risks, **saving money**.
Insurance, 5,000+ employees

Contract management and **cost reduction**.
Education, 1,001-5,000 employees

More information and **less time my employees have to spend researching**.
Credit Union, Less than $1B

Contract tracking, annual risk assessments, and due diligence gathering.
Bank, $1B to $10B

Preventing losses, both financially and in regards to data protection, to provide **confidence in our organization's processes**, and ensure successful continuity while also meeting regulatory expectations.
Credit Union, Less than $1B

Assurance.
Technology Services or Software, 1,001-5,000 employees

It allows our organization to **understand the real risk of engaging** with our third parties.
Bank, $1B to $10B

Better **recordkeeping for audit** purposes; managing risks such as cybersecurity.
Wealth/Asset Management, 501-1,000 employees

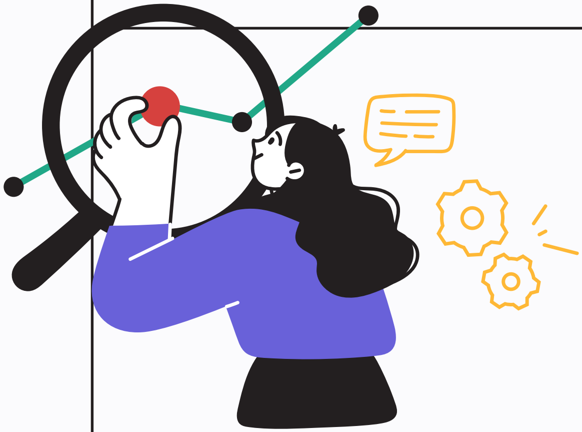
Safety, security, savings in long-term.
Fintech, 251-500 employees

Ensuring an appropriate **security** posture within risk appetite.
Bank, $1B to $10B

Helps **identify** additional **enterprise risk.**
Insurance, 251-500 employees

A **snapshot into the strengths and weaknesses** of a third party.
Credit Union, Less than $1B

Ability to **help protect the organization from initial and ongoing threats from vendors** who can be critical to our organization's overall operations.
Mortgage, 1,001-5,000 employees



Central repository, **consistency** in risk categorization, and review of the agreement.
Credit Union, $1B to $10B

Security and Safety.
Bank, $1B to $10B

Besides being compliant, **proper oversight** ensures vendors are providing the services that were contracted.
Bank, Less than $1B

Keep **track of all active contracts** we have, know who our critical vendors are and ensure we have **proper backup**, ability to quickly see which vendors have access to NPI.
Non-Financial Institution Lending, 101-250 employees

Mitigates disruption of key supplier services that could result in severe impacts to employees, revenue, and reputation/brand.
Retail, 5,000+ employees

Oversight to **identify potential risk**, ability to avoid duplication, and use the vendor product or service to its full capability.
Bank, $1B to $10B

Protects from any negative due diligence from a third-party provider.
Bank, $1B to $10B

Quality assurance, regulatory benefit, **reputation protection.**
Bank, Less than $1B

Protect the bank, **comply with regulation.**
Bank, $1B to $10B

Knowing who we do business with and what they do for us.
Bank, $1B to $10B

Keeping the **member's information safe**.
Credit Union, $1B to $10B

Resiliency, cyber/information security, best practice, regulatory.
Wealth/Asset Management, 501-1,000 employees

Risk protection and oversight.
Fintech, 101-250 employees

Regulatory governance and reputation risk mitigation.
Bank, Greater than $10B

Ensure that our service providers are **sufficiently protecting our employee and client data**. Enable our business to leverage external expertise that will allow for greater risk taking.
Wealth/Asset Management, 501-1,000 employees

Thoughtful onboarding and review of vendor management contracts and vendor relationships. **Reporting to the board and executives** and monitoring of critical and high-risk vendors.
Bank, Greater than $10B

Visibility into business relationships.
Bank, $1B to $10B

We are more **competitive** with a history of solid business relationships with **vetted teaming partners.**
Government, 5,000+ employees

Comply with regulations.
Bank, Less than $1B

Mitigating vendor risks.
Credit Union, $1B to $10B

As the primary manager of the function, it is important to have an **understanding of our third parties** and the impact they have on our operations.
Bank, Less than $1B

Reduction in risks and costs along with ability to be **proactive with cyber risks and budgeting**.
Credit Union, $1B to $10B

Protection from financial risk.
Brokerage, 1,001-5,000 employees

Meeting regulatory requirements. **Safeguarding and protecting** the organization.
Insurance, 5,000+ employees

Protect the company's data.
Logistics, $1B to $10B

Allow you to **address future risks in less time** and with **fewer resources.** Provide context for your organization and your vendors. Ensure the reputation and quality of your products and services are not damaged. Reduced costs.
Wealth/Asset Management, 5,000+ employees

Exposure to the cloud, knowing the security process/controls of our vendors, **knowing where our data is going** (personal and business).
Wealth/Asset Management, 251-500 employees

Assure that our critical and **high-risk vendors are in regulatory compliance.**
Bank, $1B to $10B

Compliance/Risk/Legal.
Bank and Mortgage, Greater than $10B

Reduce risk, helps **address future risks**, reduce costs.
Multinational Fast-Food Chain, Greater than $10B

Legal and **financial liability.**
Bank, Greater than $10B

We set barriers to **protect** the **company from malicious actions**. It is an extremely important role for a Credit Union.
Credit Union, $1B to $10B

Safeguards.
Insurance, 5,000+ employees

We work in a regulated industry, and we are ourselves subject to regulation, so I believe it for sure checks that box, but since we are trying to secure business with banks and other financial institutions, I think it **provides a sense of security** to them in engaging in a relationship with us.
Fintech, 251-500 employees

Regulatory compliance and **awareness of vendors** and their situations.
Credit Union, $1B to $10B

Reduces several risk areas (i.e., reputation, financial, regulatory).
Bank, $1B to $10B

Regulatory **compliance**.
Bank, $1B to $10B

Driving credibility for existing and potential clients. **Safeguarding** own data.
Technology Services or Software, 5,000+ employees

Avoid regulatory scrutiny. Ensure that third party relationships are positive.
Credit Union, $1B to $10B

Risk awareness and reduction plus **cost optimization.**
Insurance, 1,001-5,000 employees

Quality control and protection.
Bank, $1B to $10B

Scale, **visibility of supply chain** and third-party risk.
Fintech, 1,001-5,000 employees

Audit efficiencies.
Fintech, 251-500 employees

Avoid third-party cyber incidents. Provides regulatory requirements. Gives **reputation protection**.
Bank, $1B to $10B

Cost avoidance of legal issues.
Managed Service Provider - Human Capital Management, $1B to $10B

Meeting **regulator expectations**.
Bank, $1B to $10B

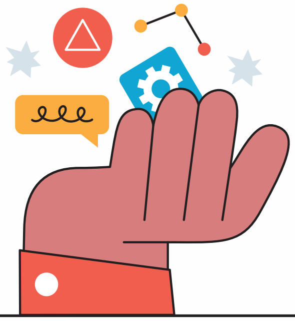
Mitigates risks with suppliers and software assets.
Technology Services or Software, 5,000+ employees

Gives guidance to the business on vendor risks.
Healthcare, 5,000+ employees

Protecting our member's information and being in compliance.
Credit Union, $1B to $10B

Understanding of **operational resistance needs**.
Bank, $1B to $10B

Third-party risk avoidance, mitigation, and resolution, as well as **strategic planning and guidance** that support a strong and effective institution.
Bank, Greater than $10B



I think it makes us manage our risk appetite and we make sure that we are compliant with industry regulations. We make sure that we **maintain a diverse supplier relationship**, which benefits not only the company, but also contribute to the society by being diverse and inclusive.
Mortgage, 5,000+ employees

Reduced costs, risk mitigation, improved performance, increased business competitiveness.
Bank, $1B to $10B

Ensure that the vendors we work with align with our values and can deliver.
Bank, $1B to $10B

Reduce risk.
Brokerage, 1,001-5,000 employees

Reduces risk for the organization.
Technology Services or Software, 501-1,000 employees

Insight into the **capabilities and health** of our vendors.
Bank, $1B to $10B

Risk management and more **effective contract management**.
Credit Union, Less than $1B

Cost effectiveness and efficiency.
Credit Union, Less than $1B

Knowing our risks; knowing our vendors business better; **compliance and regulatory needs met**.
Credit Union, $1B to $10B

Like knowing your customer (KYC), knowing your vendor and vendor's vendors is a good tool to use for **selecting the appropriate third-party vendor to ensure the product will align with the vision of the financial institution** and that the vendor is able to provide the products and services requested of them.
Bank, Less than $1B

Regulatory protection and **business protection/risk aversion**.
Bank, $1B to $10B

Risk reduction.
Manufacturing, Greater than $10B

To be in **compliance.**
Auto Finance, $1B to $10B

The **understanding into what type of vendor/partners** we are working with.
Bank, $1B to $10B

Risk and **compliance.**
Technology Services or Software, 5000+ employees

Compliance, **cost savings**, lower risk.
Healthcare, 1-1-250 employees

Overall view of the risks posed by vendors and their technologies.
Bank, $1B to $10B

Proactive information rather than reactive.
Credit Union, $1B to $10B

Operational intelligence.
Education, 1-100 employees

Compliance, risk mitigation, **good contracts.**
Bank, Greater than $10B

Protection again loss, reputation.
Mortgage, 1,001-5,000 employees

Lower costs and manage risk to an acceptable level.
Bank, Greater than $10B

Selection of best technology partners, legal and compliance protection, savings from negotiated deals, and selection of vendors through RFP process, **tracked and managed performance of suppliers** (KPIs and SLAs), much more!
Retail, 5,000+ employees

1. Creating a single source of truth for vendor information 2. Reduction of lead times through process efficiencies and the automation of vendor management steps 3. **Effective management of our ever expanding vendor population** (i.e., ESG data elements and analytics) 4. Greater visibility into, and therefore mitigation capabilities for, our vendor risks.
Bank, Greater than $10B

Adherence to **regulatory guidance.**
Bank, $1B to $10B

Decreased regulatory risk, decreased reputational risk, **lower vendor costs**.
Fintech, 251-500 employees

Better understanding of third-party services and vendors, types of data stored and accessed, **ensuring regulatory requirements are met.**
Mortage, 5,000+ employees

Ability to see across the risk landscape of our organization, proactively mitigate third party risk, **reduce impact third party risk posed to our organization,** ability to meet regulatory compliance requirements, and enhance our operational resilience.
Professional Association, Less than $1B

Recommendations and Best Practices

As in previous years, the importance of third-party risk management keeps rising. Regardless of your organization's size or industry, we have all faced third-party risk management challenges, but we have also had the chance to grow. Maintaining awareness of what is happening in the third-party risk management industry and keeping your ears open are the best ways to anticipate what might be ahead. But, what can third-party risk management practitioners do to maintain effective programs and keep risk at bay?

No matter how effective and mature your program may be, there is always room for improvement. Take time to thoroughly review your program to identify any gaps or weaknesses, prioritize areas for improvement, and document your plans to implement them.

As we move into 2023, here are some third-party risk management best practices to consider:

BEST PRACTICES FOR 2023

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 document requirements up to date and relevant to the current risk environment.
4. 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.
5. Monitor and track vendor issues through remediation.
6. Measure the impact of third-party risk management through program metrics and reviews.
7. Keep senior management well informed.
8. Stay on top of the industry news and enforcement actions.

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
Twitter
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

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.