venminder

State of Third-Party Risk Management

2022 Whitepaper

Copyright © 2022 Venminder, Inc

Table of Contents

Copyright © 2022 Venminder, Inc

Executive Summary

Venminder's State of Third-Party Risk Management 2022 survey provides insight into how organizations manage third-party risk today.

The survey results allow for a deeper look into current practices, shared challenges, incentives for compliance and benefits of third-party risk management.

This is Venminder's sixth annual whitepaper that surveyed individuals from a wide variety of organizations and industries including financial services, fintech, retail, insurance, healthcare, information technology and more.

Venminder promoted the survey publicly through email, social media and the Third-Party ThinkTank online community November 2021 through January 2022. To provide confidence in the validity of responses, participants were allowed to provide anonymous and confidential answers.

While not as volatile as the year preceding it, 2021 brought us closer to what might become our "new normal." Despite the broad distributions of COVID-19 vaccines, organizations everywhere faced uncertainty as the pandemic continued, cybercrime exploded, supply chains were interrupted and millions of workers resigned. In the face of all this change, we were continuously reminded of the importance of effective third-party risk management (TPRM). TPRM practitioners continued to answer the call and have shared their experiences and insight with us.

Thank you to everyone who participated in this year's survey. Your contributions help inform a broad array of industries on the challenges and opportunities of TPRM.

Copyright © 2022 Venminder, Inc

Survey Highlights

Venminder's State of Third-Party Risk Management 2022 survey provides insights that allow for peer-to-peer learning and the ability to benchmark against current best practices.

Here are just a few survey highlights:

1

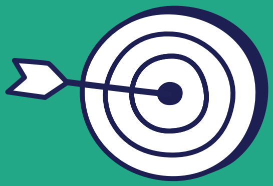
Vendor risk management programs are still ***understaffed*** *and* ***underfunded***

2

Cybersecurity *is a top concern*

3

The majority of programs are now using ***dedicated vendor risk management systems***



4

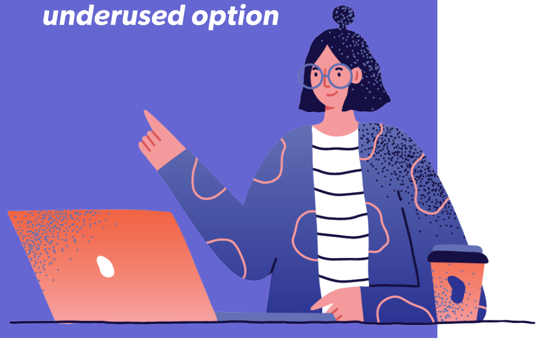
Programs are feeling more ***scrutiny from auditors and examiners***

5

Vendor business continuity planning (BCP) ***saves the day***

6

Outsourcing is a viable but ***underused option***



Copyright © 2022 Venminder, Inc

Survey Results

Copyright © 2022 Venminder, Inc

Commitment to Vendor Management

Internal Resources Committed to Vendor Management

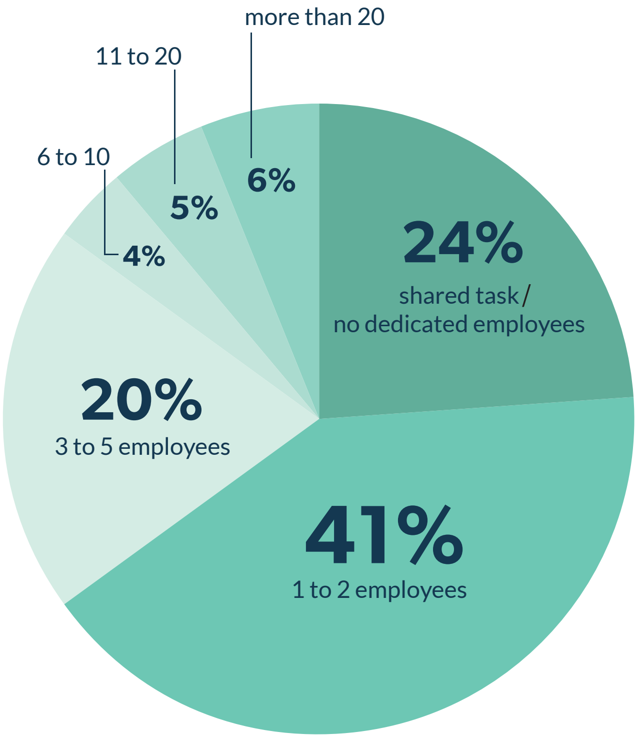
Real concerns in certain areas

Twenty-four percent (24%) of organizations reported having no dedicated vendor management employees and were relying on existing employees to share the workload. That number has been minimally reduced compared to the previous year's twenty-six percent (26%).

The good news is that most organizations are reporting that they do have dedicated employees to run their vendor management programs. Forty-one percent (41%) responded that they have 1-2 employees, which remains the same as the previous year. The increase to 20% of respondents reporting 3-5 employees is encouraging, as last year the number was fifteen percent. Four percent (4%) of organizations have 6-10 employees. The remaining 11% have more than 10 employees.

There are, of course, several factors that go into determining the correct number of dedicated employees for any third-party risk management (TPRM) program. Mature programs that take advantage of automation through TPRM software, have engaged and compliant vendor owners and implement effective processes can undoubtedly get the job done with fewer dedicated people. Still, nearly half of our respondents operate with two or fewer dedicated employees.

How many full-time employees are dedicated to your vendor management program?

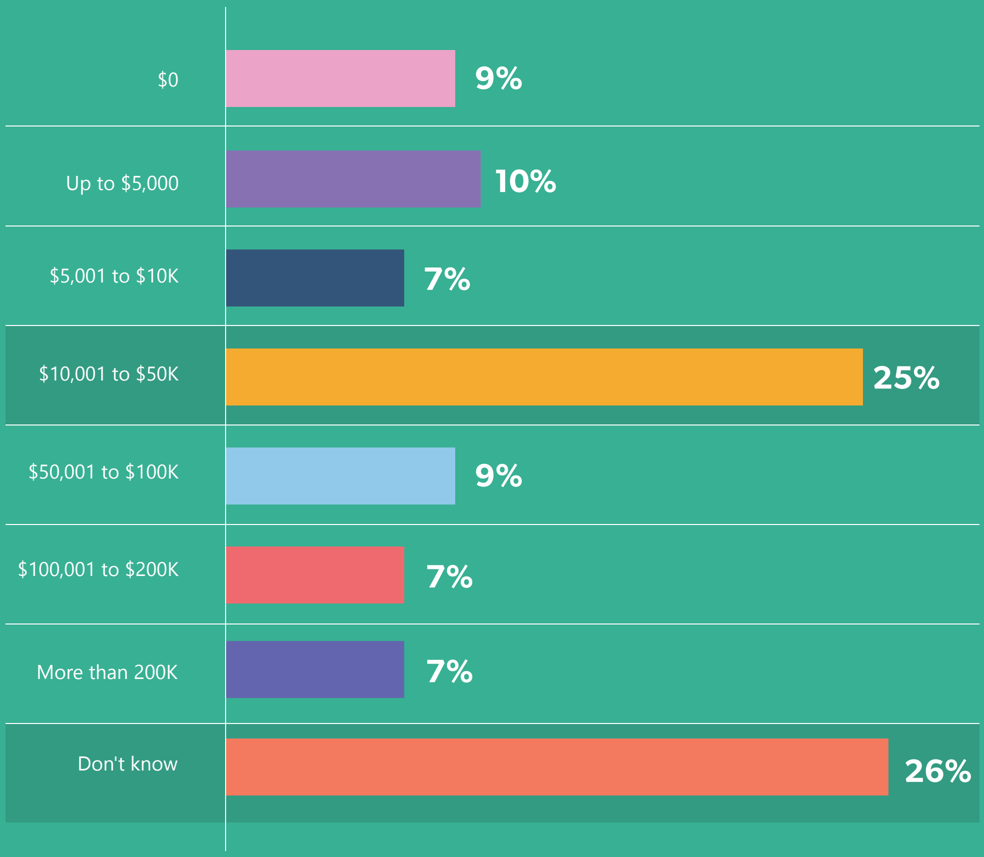


Copyright © 2022 Venminder, Inc

Even the most optimized programs still have a large amount of work to get done, and there are limitations to what even the most adept TPRM professional can accomplish in a day. Understaffed programs result in overworked and stressed employees, increased errors, overlooked risks, longer processing times, frustrated lines of business, unhappy vendors and potential regulatory findings.

Ensuring that a TPRM program is adequately staffed with skilled personnel is essential for its success.

Besides full-time employee costs, how much budget has been dedicated to vendor management?



Copyright © 2022 Venminder, Inc

Program investment has increased slightly as only 26% of programs still spend less than $10,000. Forty-eight percent (48%) of respondents reported spending more than $10,000. These nominal increases are still encouraging, considering the additional budget stresses and financial pressures most organizations underwent this past year. We anticipate seeing these increase as the business environment stabilizes and regulatory pressures intensify.

Allocating enough program dollars is essential to ensure a consistent and well-run program. At a minimum, funding should adequately support dedicated staff and TPRM technology. Good budgeting can help ensure a well-run and effective program. Investments in additional staff, external advice, legal opinions, risk alert monitoring services and even outsourcing portions of the TPRM process can enhance the program and optimize the time available for staff to focus on identifying and managing risks.

The long-tail effects of the pandemic, worker shortages, an active regulatory environment and the rapid expansion of third-party risks ***all justify additional program funding****.*

This is especially true for organizations that can't dedicate full-time staff to TPRM. Investments of $50,000 or more appear reasonable for most regulated organizations.

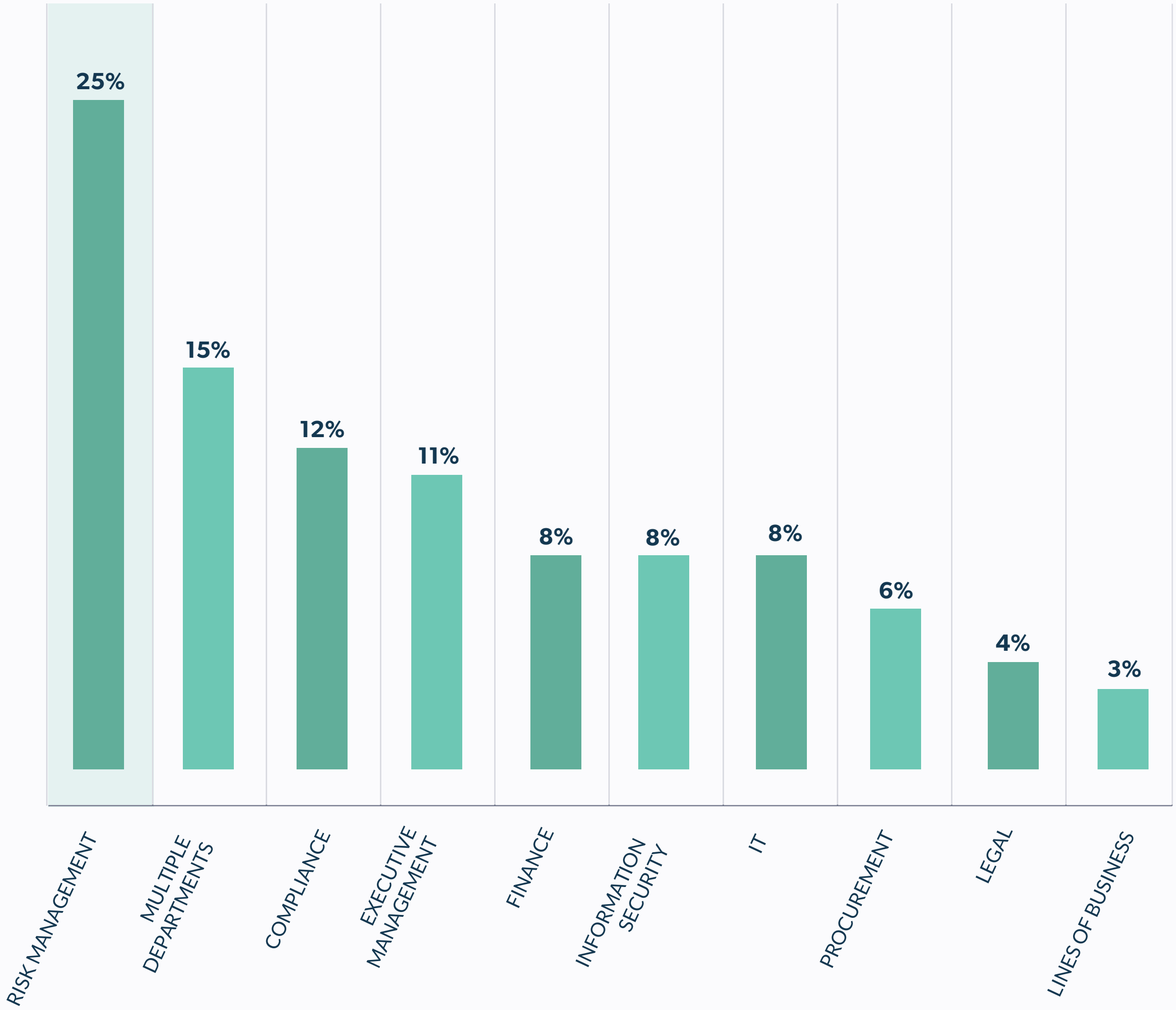
Copyright © 2022 Venminder, Inc

Organizational Structure

Independence from lines of business continues as a trend

TPRM continues to be housed under different internal organizations but has largely moved away from the lines of business. Consistent with previous years, most respondents (37%) report into risk or compliance organizations, reflecting TPRM as a proper risk discipline and practice. Reporting to multiple departments seems to be a growing trend (15% compared to 10% in 2020). Finance and IT have seen slight increases since 2021, with IT representing 8% vs. 3% a year ago and finance representing 8% now, vs. 6% a year ago.

Where does vendor management report to?



Copyright © 2022 Venminder, Inc

Most importantly, TPRM moving away from the lines of business enables it to work with more neutrality and independence. Separation of duties is an essential component of an effective TPRM program. TPRM must be allowed to apply the process impartially without the potential conflict between meeting department goals and third-party risk objectives.

> *Before finding a permanent home, organizations with newer TPRM programs often go through multiple internal organizational alignments.*

EXAMPLE

Here's an example: it's not uncommon for the TPRM function to begin as an offshoot of information security. It could then move on to another department when there's an increased understanding that TPRM is meant to identify and manage risks beyond those of just an information security nature. Best practices dictate that TPRM is aligned to the organization's risk function, such as enterprise risk management or risk and compliance, as these functions have similar goals and compatible objectives.

> *Regardless of where the TPRM function sits, **senior leadership must demonstrate their understanding of its purpose and objectives** by providing sufficient resources, support and sponsorship.*

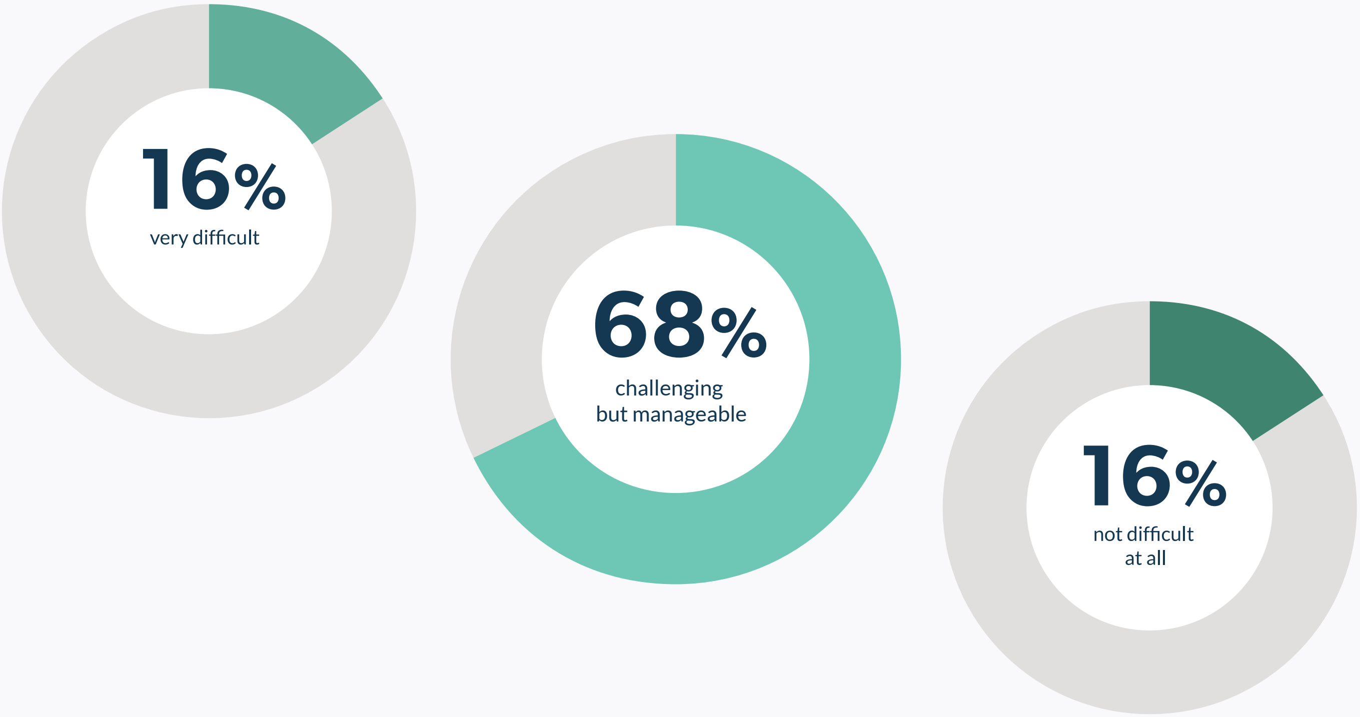
Sponsorship from the Top

Setting the tone from the top is important

Among TRPM concerns, securing business unit and vendor owner support remains a consistent challenge. Many TPRM teams will tell you that friction with the business line or vendor owner can be stressful and a barrier to the program's effectiveness. Sometimes TPRM activities are not prioritized by the business lines or are treated as secondary to what the business may see as their objectives. In other cases, there may be pushback from the business line or vendor owner who may disagree with their designated role and responsibilities as part of the TPRM process. Often, TPRM teams may find they must constantly follow up on late or missing vendor owner deliverables. In some organizations, process changes or new requirements are met with resistance or ignored by the business lines. Unfortunately, these scenarios are painfully familiar for many TPRM teams.

Similar to previous years, 68% of our respondents found that getting the line of business or vendor owner support is challenging, but manageable, and 16% found it very difficult. Still, there is that fortunate 16% of respondents that didn't find if difficult at all.

How difficult is it to secure business unit support for your vendor management program requirements?



Copyright © 2022 Venminder, Inc

Typically, when TPRM faces these challenges, the underlying problem is frequently the "tone from the top." Senior leadership may not realize that they have a fundamental role in the effectiveness of the organization's TPRM program. What they do and say matters and has a domino effect down through the organization. When TPRM programs are poorly funded and without enough resources, the unspoken message is that it must not be a priority.

> *When the business lines are out of compliance with TPRM requirements and leadership seems unconcerned, the unspoken message is that TPRM is another "check-the-box" activity.*

On the contrary, the whole organization notices when the board and senior leadership take an active position by incorporating TPRM into strategic planning and decision-making. Furthermore, ensuring that TPRM programs are appropriately funded, have adequate resources and have the autonomy and independence to perform their roles demonstrates that it's an essential function. Finally, senior leadership needs to champion TPRM and treat it with the same consideration and importance as other risk functions.

Copyright © 2022 Venminder, Inc

Vendor Management Processes

Copyright © 2022 Venminder, Inc

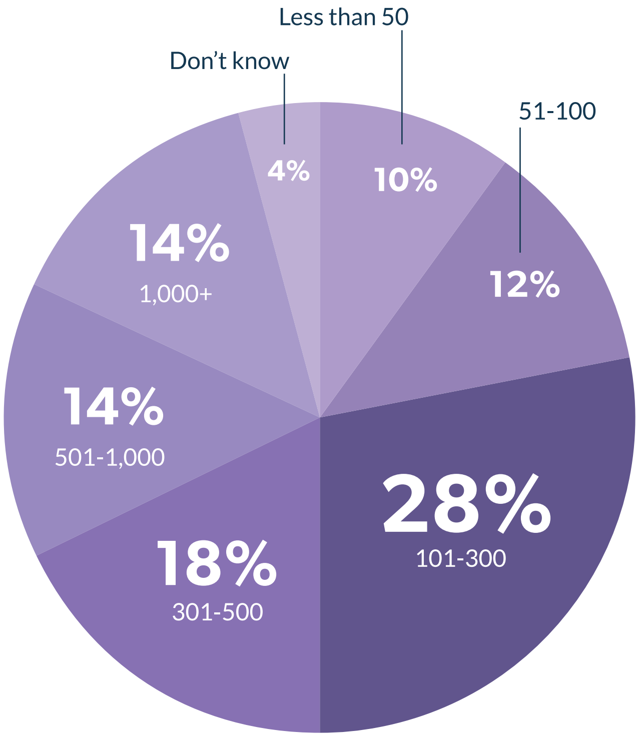
Size and Makeup of Vendor Landscape

At most organizations, vendor management is complex

Outsourcing strategies vary, with some organizations choosing to outsource almost everything. In contrast, others take a more conservative approach, preferring to keep most activities in-house. No two organizations are the same and the number of third parties under management isn't necessarily related to the organization's size.

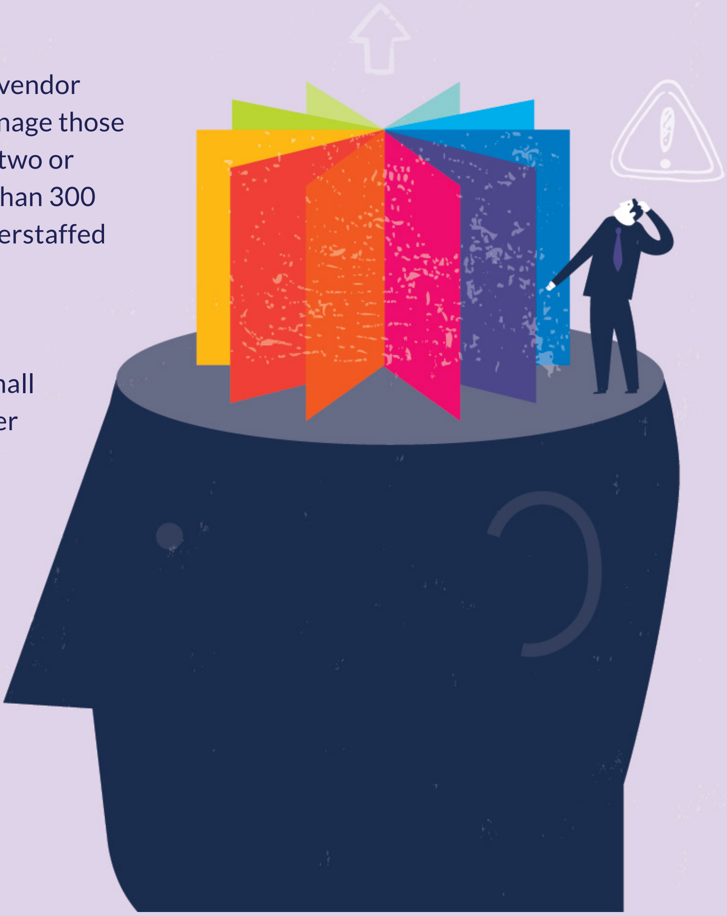
Our survey sample showed that 10% of our respondents had less than 50 vendors and 12% had 51-100 vendors. It seems that most programs fall in the mid-size range, with 28% reporting 101-300 vendors and another 18% citing 301-500 vendors. Fourteen percent (14%) of our respondents report more extensive vendor inventories of 501-1,000 vendors. Another 14% reported more than 1,000 vendors, a slight increase from the previous year of thirteen percent (13%). The good news is that only 4% didn't know how many vendors they had. It's essential to have an accurate vendor inventory to identify the risk's scope and size. Again, the number of vendors isn't always reflective of an organization's size.

How many total vendors are included in your vendor management program?



Copyright © 2022 Venminder, Inc

But, what can the size of your vendor inventory tell you?



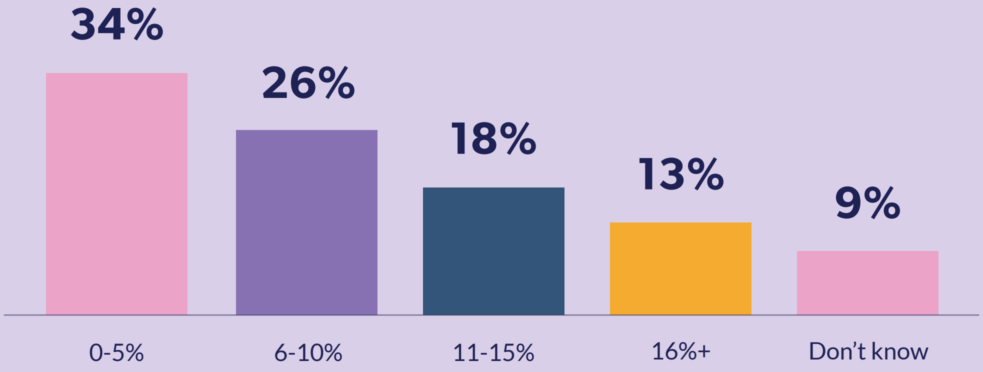
First, it's helpful to understand the amount of risk in your vendor inventory to estimate how much effort is necessary to manage those risks. Remember, 65% of our survey sample said they had two or fewer dedicated employees, but 46% said they had more than 300 vendors. That set of data points can tell us a lot about understaffed TPRM teams.

Second, the size of the list can be an indicator of effective TPRM and procurement processes. Suppose you have a small organization, but a huge vendor list. When you take a closer look, there might be vendors with expired contracts or those still billing you for products and services you don't actually receive. From another perspective, let's say that 15% of the vendors on your list sell office supplies. That may indicate that your organization isn't leveraging any volume discounts or has no real 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 may be looking at a severe concentration risk.

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

What matters most is that your vendor list is accurate and reflects which products and services are being provided to your organization, vendors are correctly risk rated and critical vendors are clearly identified.

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



Copyright © 2022 Venminder, Inc

More than half (60%) of our respondents tell us that critical vendors make up 10% or less of their total vendor population, which is in line with best practices. Still, nearly a third of those surveyed (31%) reported critical vendors making up 11% (or more) of their vendor inventories. One possible reason for those more significant percentages might be that some organizations use critical as a risk rating vs. an indicator of business impact. That particular misunderstanding is relatively widespread and usually results in too many vendors being labeled critical.

In fact, every vendor should be considered either critical or non-critical. Following that practice will help you define which vendors can severely impact or shut down your essential operational processes and functions should they fail. Critical vendors are often also high-risk, but not all high-risk vendors are considered critical.

The definition of "critical" can sometimes vary, but this 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 any of these are "yes," that should be considered a critical vendor.

Determining vendor criticality is essential, as it drives deeper due diligence, requires carefully written contracts and requires consideration of what must be done to minimize disruption to your business and your customers in the event of a vendor failure.

Copyright © 2022 Venminder, Inc

Operating Models

Hybrid models are on the rise

There's more than one vendor management model, and organizations may try one or more before they find the operating model that works best. We wanted to know how our participants approached vendor management and asked which of the three models they use:

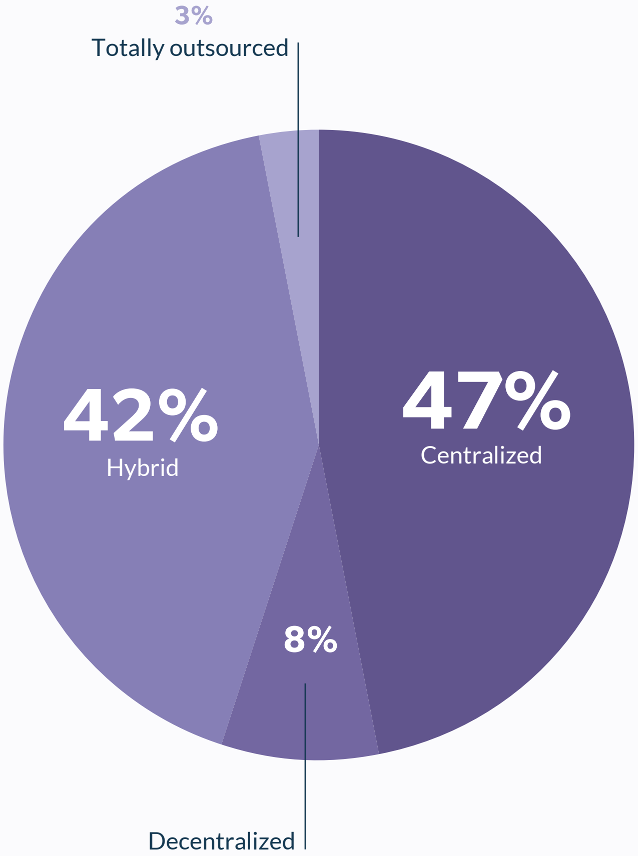
EXAMPLE

Centralized: All TPRM functions are conducted by the same dedicated team

Hybrid: Shared functions between a dedicated team and other departments

Decentralized: Functions are managed across teams without any dedicated team

What operating model do you use for your vendor management program?



Copyright © 2022 Venminder, Inc

Centralized models are still the most popular, with 47% reporting their use in the last year. This model is declining, as it is down from 54% in the previous year. Centralized models are practical and effective because responsibility and accountability are housed in one place. The tasks required are completed by knowledgeable individuals familiar with the work and experienced in the processes. However, there are some downsides. One is that the true vendor owner, usually in the business line, isn't fully engaged in managing the risk, resulting 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 increasing**. Forty-two percent (42%) of our respondents reported using a hybrid model, up from 34% in the previous year. Hybrid models work well as there is a dedicated team to maintain the program's structure and flow, keep everyone on task and accountable and provide reporting. Individual risk owners are 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.

There's often **inconsistency in fulfilling vendor risk requirements in a decentralized model** (used by 8% of our sample) and reporting and documentation are often hard to gather or are incomplete. Also, the additional TPRM tasks aren't always prioritized against other business objectives and are often left undone. Many programs begin using a decentralized model but move away from it when the need to optimize becomes apparent.

> *Outsourcing portions of the TPRM process, such as due diligence document collection and subject matter expert reviews, is becoming a popular option for some organizations.*

In fact, some of the major regulators have voiced support for outsourcing due diligence if your organization doesn't have enough skilled resources. However, completely outsourcing TPRM, as 3% of our respondents do, can cause more problems than it can solve. TPRM requires a solid internal view and understanding of the products and services provided by the vendors and the risks presented by them. Removing the internal risk management responsibilities can create a false sense of security and emerging risks are often overlooked. While outsourcing can and does make sense for many organizations, be cautious about outsourcing your whole program. When senior leadership or the board has an urgent third-party risk question, no one wants to respond with, "I'll need to call our third-party risk service provider to get that information."

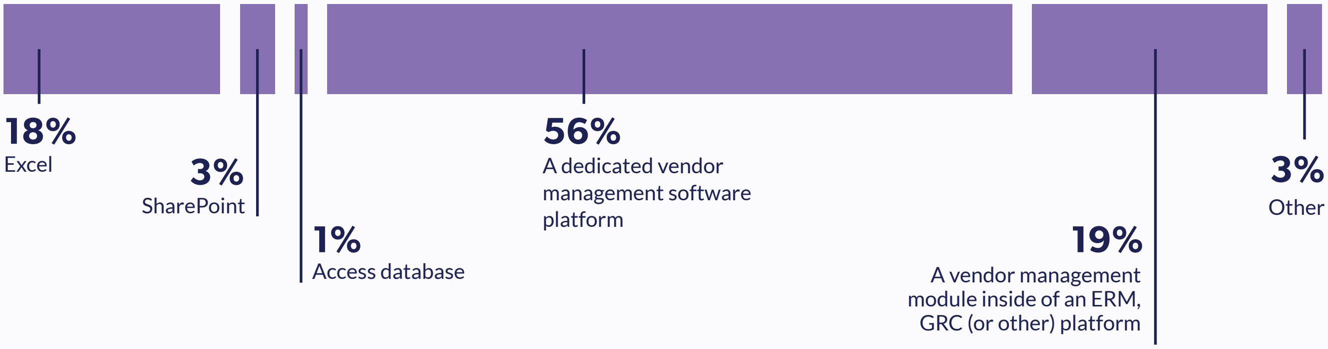
Copyright © 2022 Venminder, Inc

Technology Tools Used

A high number using dedicated platforms

There are many ways that organizations approach the management and record-keeping for the data, tasks, assessments and questionnaires, risk reviews, documents and contracts involved in vendor risk management. Eighteen percent (18%) of our respondents use Excel, 3% use SharePoint and 1% use an access database. Another 3% are using other means, possibly even homegrown solutions.

What is your primary tool for managing your vendors?



Beyond spreadsheets and databases, many solutions are being offered on the market but they aren't necessarily designed explicitly for TPRM. Remember that enterprise risk management (ERM) or governance, risk management and compliance (GRC) applications are often built to manage the organization's overall risk and aren't always equipped to manage the complex and often specialized assessment requirements associated with outsourcing.

Nineteen percent (19%) of those surveyed report using a vendor management module within another system. However, more than half (56%) of those surveyed report using dedicated vendor management software.

Dedicated vendor risk platforms are designed to address the many processes and complexities falling under the vendor risk management umbrella. They enable specific tasks, assessments, reviews and data collection across the organization and throughout the vendor risk management lifecycle. Since these vendor risk management platforms are designed to make vendor risk management more accessible and more effective, there's no need to create workarounds or repurpose other functionality in hopes that it "might work" to achieve the task at hand.

Copyright © 2022 Venminder, Inc

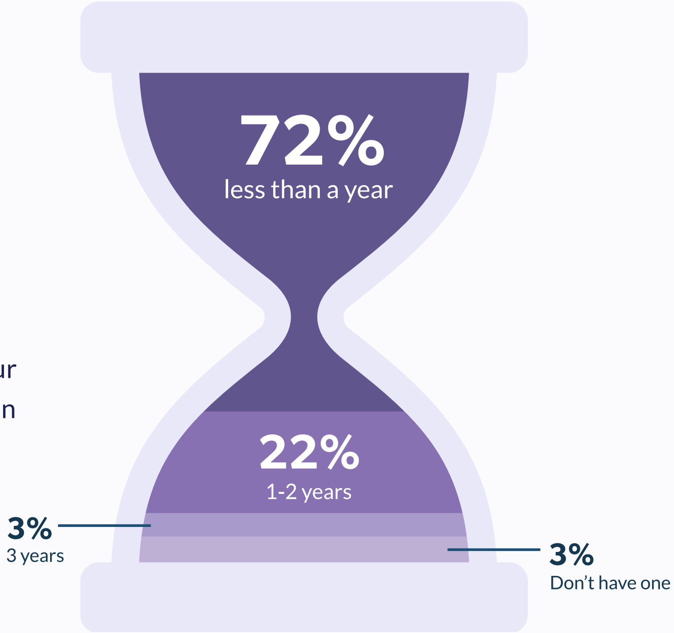
Best Practices in Vendor Management

A story in continued improvement

Your vendor management policy documents are the foundation of your program. Vendor management policy documents that are kept current and are consistent with regulatory guidance and best practices are the cornerstone of a successful TPRM program. It's good to see that the vast majority of our respondents (72%) follow these guidelines.

When was the last time you updated your vendor management policy document?

Remember, your policy should be updated at least annually, but should also be updated when there is new regulatory guidance or significant changes in your program. Auditors and regulatory examiners will often record findings for outdated policies.

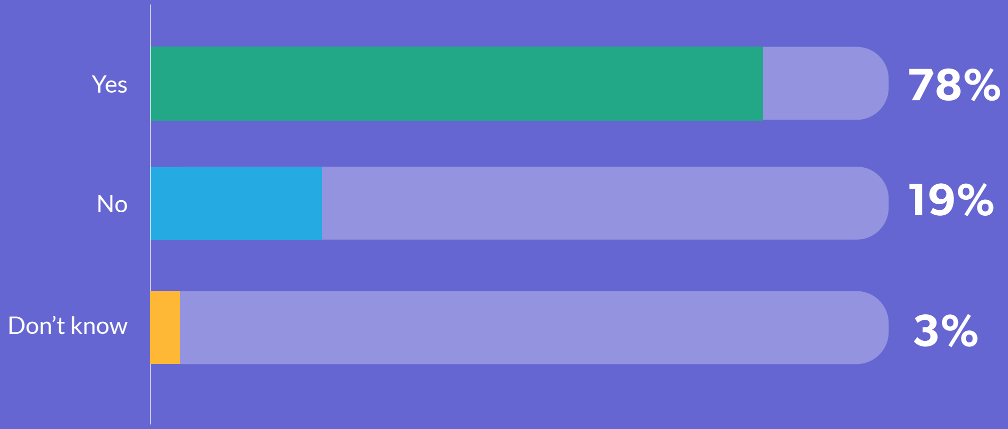


Trending up from last year, 78% of our survey sample now report having a formal process in place that determines inherent and residual risk. As the inherent risk determines the appropriate risk management requirements and activities, it's exciting to see most organizations grounded in this essential process. It is consistent with best practices and reflective of regulatory requirements.

Still, 19% don't have these formal processes in place. Hopefully, that number will decline as programs improve and mature.

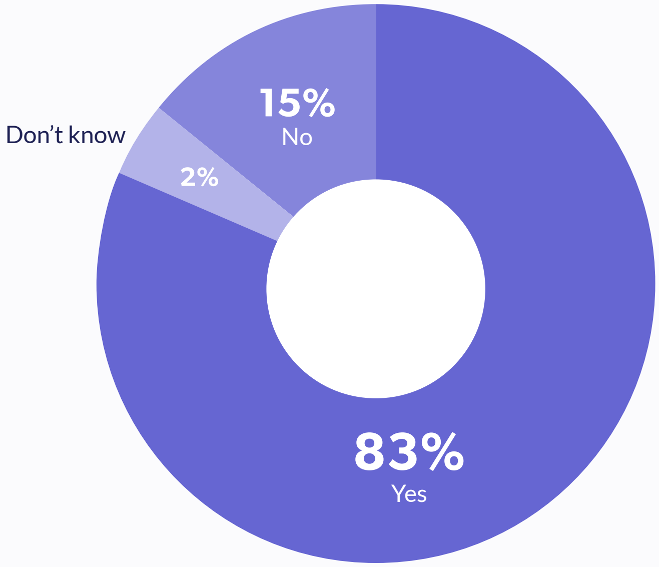
Copyright © 2022 Venminder, Inc

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



Eighty-three percent (83%) of responding organizations have shared that they have a formal process in place to identify the business impact or criticality of their vendors pre-contract. This number is up slightly from last year's 80% figure. This is also the second year in a row that the number of organizations determining criticality is higher than the number of organizations with a formal inherent risk assessment process. When we consider program maturity, we have seen a decline in the percentage of respondents with no program in place and an increase for those establishing and implementing their TPRM programs. It makes sense that many may be working to identify their critical vendors as a first step.

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



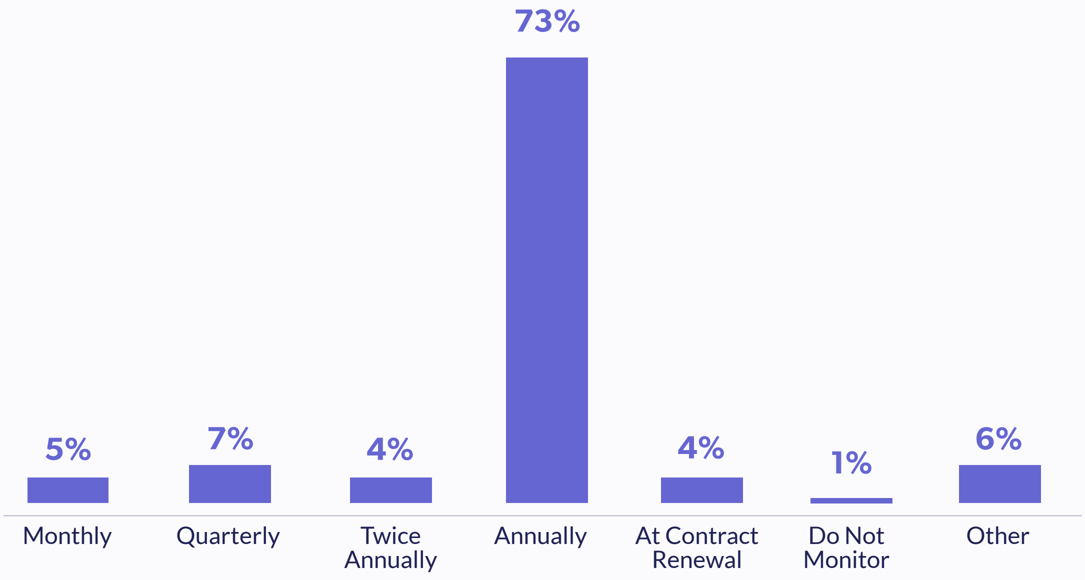
Copyright © 2022 Venminder, Inc

As a reminder, criticality and risk are NOT synonymous. Criticality speaks to business impact and risk ratings identify the types and amount of risk present in a vendor engagement.

This year, 73% of respondents said they're reviewing their high-risk or critical vendors at least annually, which is the recommended minimum. While this number is down a few points from the previous year (76%), those monitoring on a more frequent basis (5% monthly and 7% quarterly) has increased. This illustrates that organizations are committed and are even becoming more serious about monitoring critical and high-risk vendors.

Periodic assessments of your vendor's control environment are fundamental to the TPRM process, especially for critical or inherently high-risk vendors. Risk profiles can change rapidly and waiting too long between reviews or reviewing only at contract renewal increases the likelihood of new or emerging risks going unnoticed until it's too late. Remember, risk doesn't follow a calendar and can pop up at any time. Risk monitoring is never just a "one-and-done" exercise, and the frequency of those "periodic" reviews should always reflect the risk and criticality of the vendor engagement.

How often are you reviewing/analyzing your high-risk or critical vendor documentation?



Copyright © 2022 Venminder, Inc

Since the start of the pandemic, we've seen existing third-party risks grow exponentially and new risks emerge.

EXAMPLE

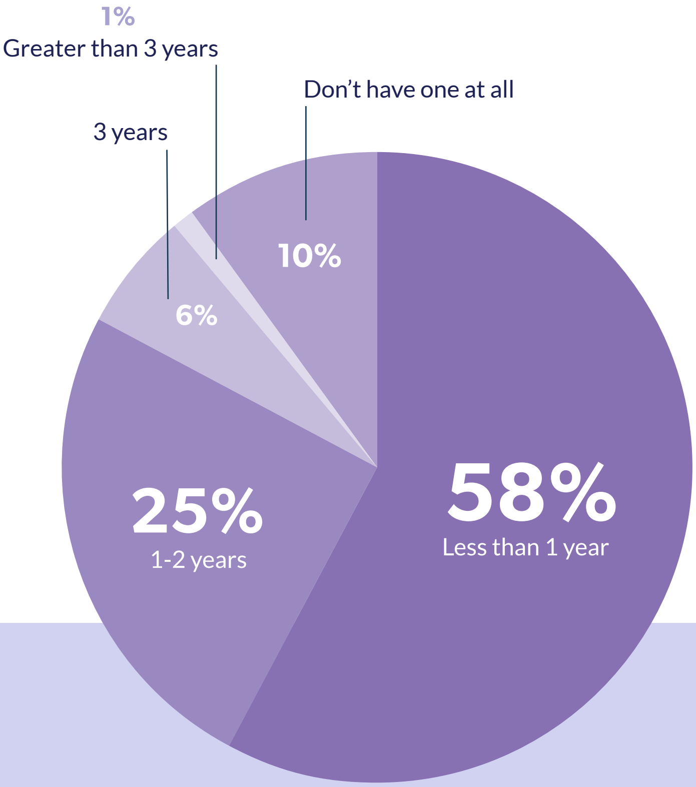
For example, according to a study by Check Point Research, reported cybercrimes and data breaches increased 50% in 2021, and Gartner's Emerging Risks Monitoring Report revealed that ransomware rapidly became a top concern within a year. As we consider the new risk environment, we wanted to understand if those new and emerging risks were being captured in inherent vendor risk assessments.

Copyright © 2022 Venminder, Inc

Your risk management is only as good as your risk identification, and risks that go unidentified go unmanaged. Fifty-eight percent (58%) of our respondents seem to agree and have updated their inherent risk assessments within the last year. Twenty-five percent (25%) have reported an update within the last 1-2 years.

Those who have not updated their inherent risk assessments in the last three years (6%) or have no inherent risk assessments at all (10%) run the risk of unidentified new and emerging risks. Remember, your inherent risk assessment should reflect the current risk environment.

How recently have you updated your inherent vendor risk assessment?



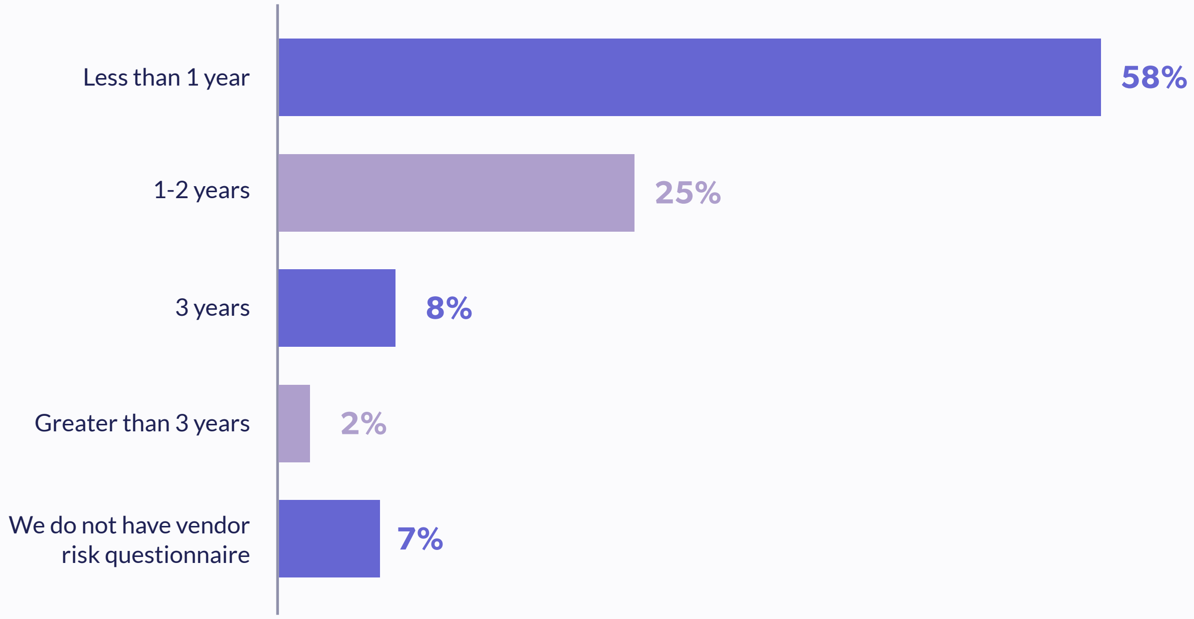
Collaborate with your subject matter experts to ***review and update your inherent risk assessments*** *at least once a year.*

Copyright © 2022 Venminder, Inc

Like your inherent risk assessment, your vendor risk questionnaire and document requests should be reviewed and updated at least once a year. Vendors are unlikely to proactively disclose information that isn't requested. Furthermore, incomplete or outdated questionnaires and document requests may send the wrong message. Your vendors may infer that your program standards are a bit too relaxed, so maybe they can be too.

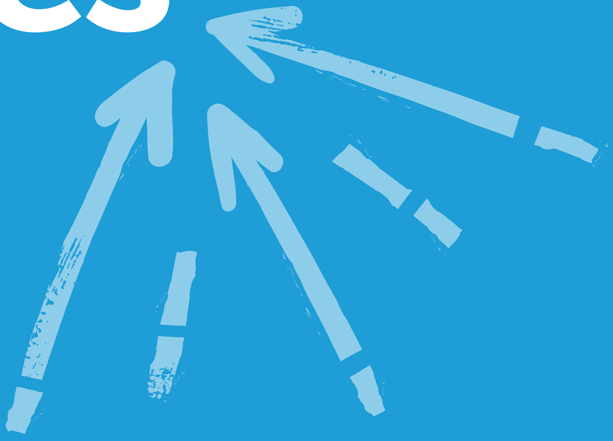
Fortunately, most of our survey participants are on top of it. Fifty-eight percent (58%) reported updates within the last year and 25% within 1-2 years. As for those who don't have any or haven't updated their risk questionnaires and document requests in more than three years, it's past time to get started. If you need any incentive to get busy, consider what has changed in the last three years. We're in a long pandemic. Millions of employee are now working from home. Cybercrime and data breaches have exploded and security features and requirements for "the cloud" have changed.
As a best practice, your vendor risk questionnaires and document requests should be reviewed (and updated if necessary) at least once a year or when there are new material risk issues or regulatory changes.

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



Copyright © 2022 Venminder, Inc

Third-Party Risk Management Growth and Pressures



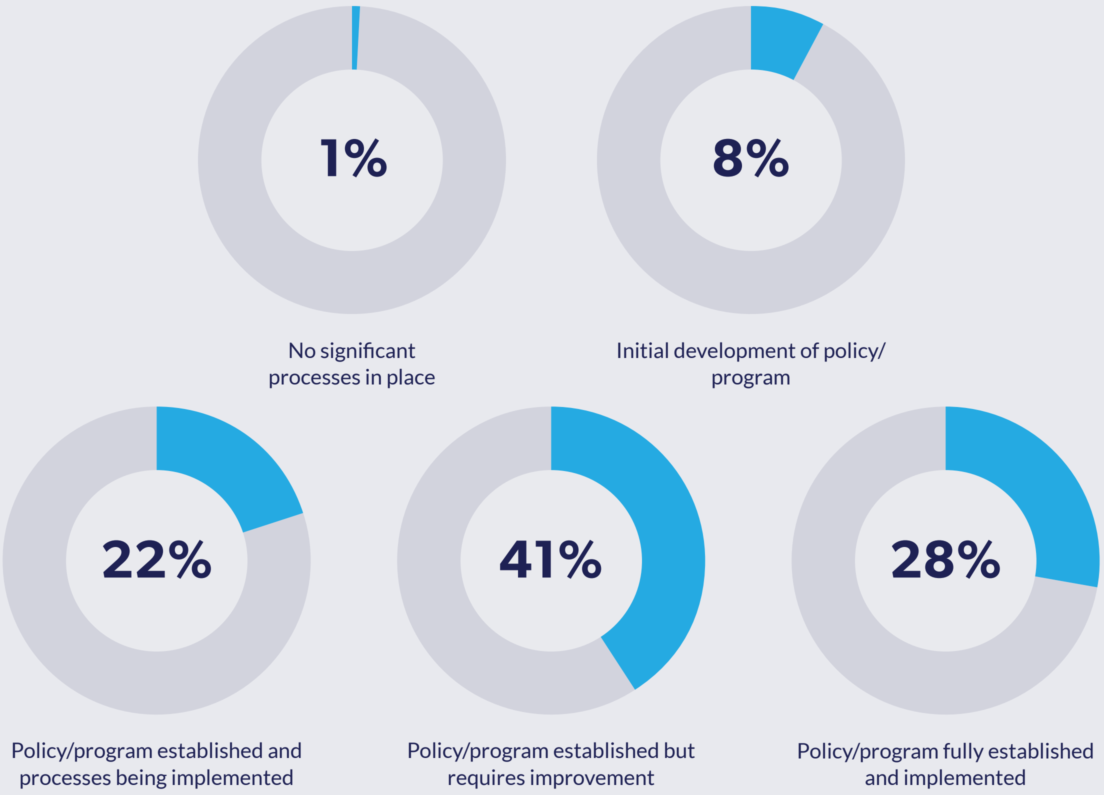
Copyright © 2022 Venminder, Inc

Maturity of Vendor Management Programs

Progress and optimization are on the rise

TPRM program maturity is improving and mature programs continue to improve. While 28% of our respondents have a fully established and implemented program, another 41% of those surveyed reported a fully established program that requires improvement. It's terrific to see the focus on improving existing programs because constant improvement is the foundation of maturity.

What would you estimate is the maturity level of your vendor management program?



Copyright © 2022 Venminder, Inc

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

- Core program documents, such as the policy and procedures, are **outdated or your procedures are hard for users to follow**
- You have clunky workflows that **confuse the users**
- **Low program compliance** and too many late or poor quality vendor risk management deliverables
- **Low quality or no reporting** for the stakeholders
- **Your inherent risk and vendor due diligence questionnaires aren't current enough** or have poorly stated questions that always require additional explanations to the vendor or vendor owners

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

Another positive factor is the increase in respondents currently establishing programs (22%) or are in initial development (8%). Finally, only 1% of those surveyed said they had no significant processes in place, down from 4% in the previous year.

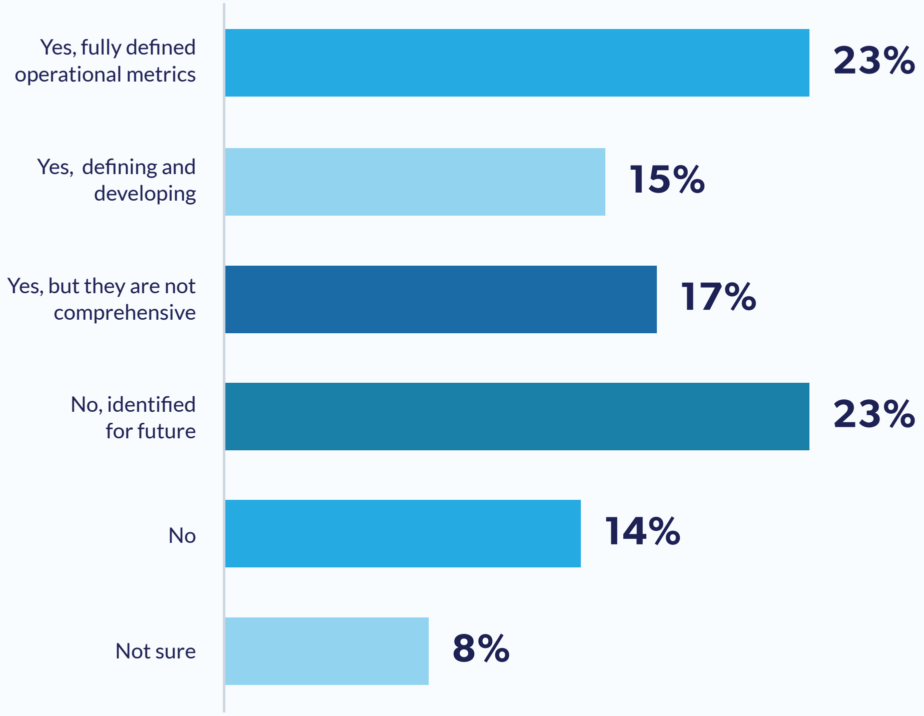
Copyright © 2022 Venminder, Inc

TPRM is a regulatory requirement for many. Still, simply having a program and going through the motions isn't enough. Understanding your program's effectiveness is essential, and confirming that TPRM's foundational objectives are being met is equally as important. Establishing a set of program metrics is the best way to holistically evaluate and measure your program's health, stability and effectiveness.

Program metrics are a hot topic right now. Many programs are looking for tools and methods to confirm the value TPRM brings to the organization, measure the program's effectiveness and benchmark against best practices.

Our survey showed that 23% of our sample have fully defined operational metrics. In comparison, another 23% said they intend to develop them in the future, while 14% had no program metrics at all. The remaining organizations fall somewhere in the middle. Seventeen percent (17%) indicated that they had some metrics, but they weren't comprehensive, and another 15% were currently developing their metrics.

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



Copyright © 2022 Venminder, Inc

It's recommended that your metrics 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 might 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 TPRM team capacity and the number of critical and high-risk vendors under management.*

Other suggested stability metrics include the number of vendor owners that have been trained in TPRM 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 TPRM narrative and ongoing value statement**.*

Copyright © 2022 Venminder, Inc

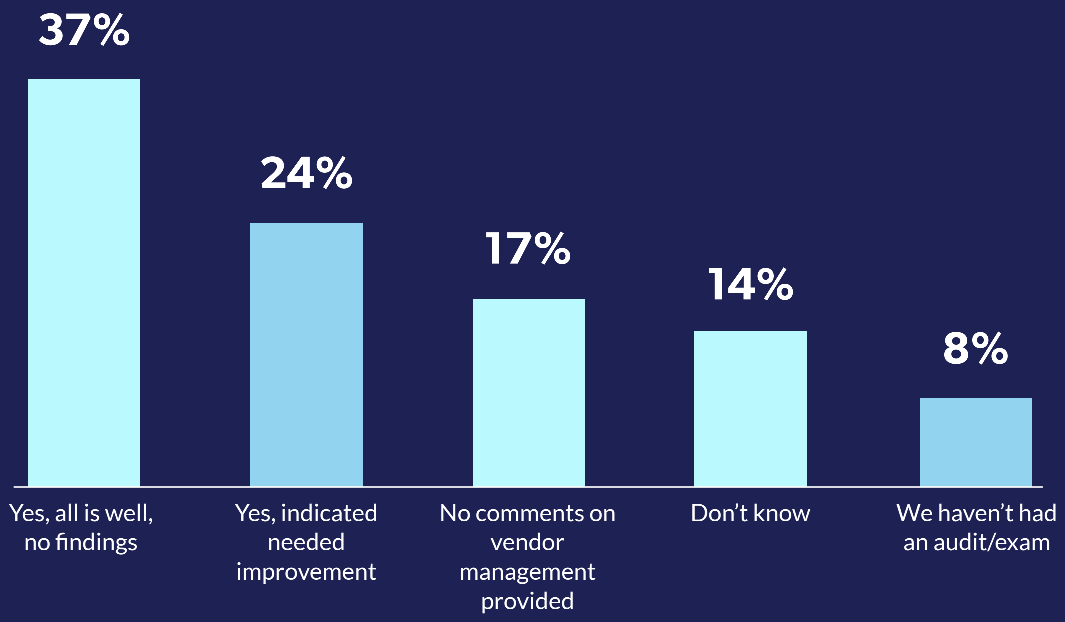
Regulatory Focus and Exams/Audit Results

Evidence of continued regulatory focus on vendor management

Audits and regulatory examinations are standard, so anticipating and preparing for them should be part of your TPRM routine. While audits and exams are the formal reviews of your program, it's best to self-audit your program frequently.

More than a third (37%) of surveyed organizations had audits or exams with no findings this year. Conversely, 24% had audits and exams with findings indicating improvement was necessary and 17% reported no comments on vendor management provided. The number of respondents who didn't know had increased (14% compared to 8% in the previous year) and 8% had not had an audit/exam in the past year.

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

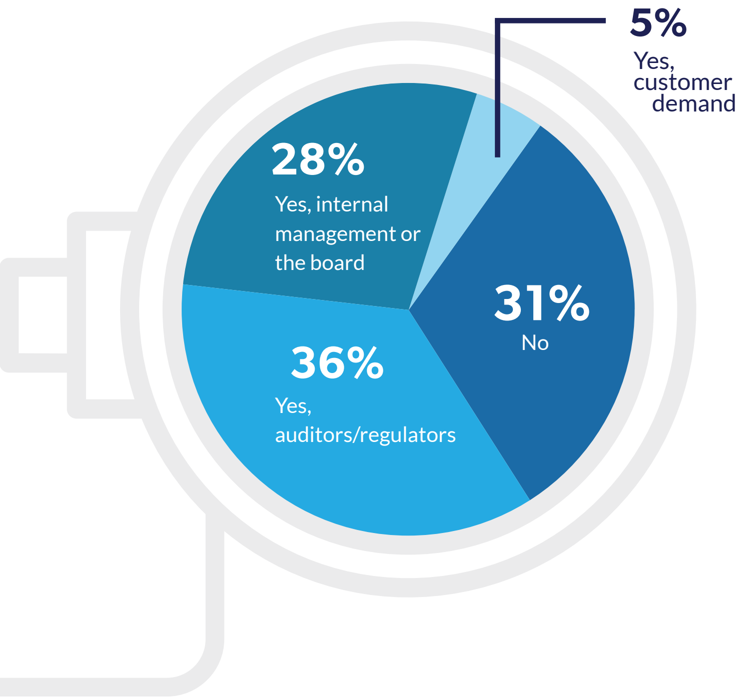


Copyright © 2022 Venminder, Inc

When auditing your TPRM program, it's essential to consider a few core requirements. First, is the policy current and aligned with all rules, laws and regulations? Second, do your actual TPRM processes align with the stated policy? If you have a requirement in the policy that isn't being followed in practice, that should be a red flag. Third, are the processes and tools effective in identifying, assessing and managing risk? Finally, are processes executed consistently and are exceptions documented?

While not a comprehensive list of requirements, evaluating your program considering the questions above will help you identify program gaps or weaknesses. It will also indicate where you can make program improvements before your auditor or examiner begins their review.

Are you feeling pressure to improve your vendor management program? If yes, what is the most significant source?



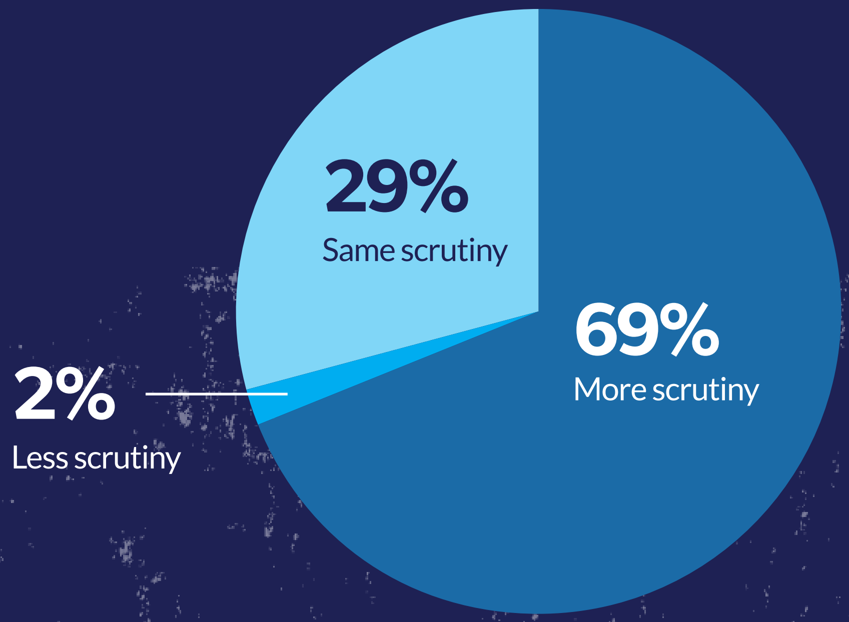
Interestingly, almost a third (31%) of our sample said they weren't feeling any pressure to improve their program, which is surprising since a cumulative 64% said they were feeling pressure from auditors and regulators (36%) or internally from the board or senior management (28%). Customers (5%) also demand better TPRM.

There is no real news here. The pressure to keep vendor management current with evolving regulations, the expansion of vendor risks and an increasing need to keep customer data safe, is ongoing. The best and most effective programs practice continuous improvement.

It makes sense that 69% of respondents felt more pressure from auditors and regulators over the last year. Since 2020, the regulatory environment has started to move again after what seemed to be a long rest. New presidential administrations, the pandemic, the rise of new technologies, the increase of cybercrime and data breaches and the growing demand from investors and consumers for ESG (environmental, social and governance) transparency have created quite a long list to be addressed by regulators and lawmakers.

Copyright © 2022 Venminder, Inc

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



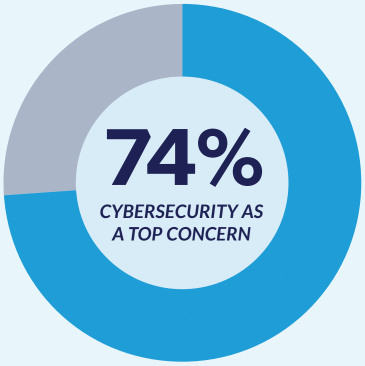
New or Emerging Vendor Risk

Cybersecurity incidents are rising in frequency and complexity

Many organizations have felt a seismic shift lately regarding vendor risk. Not only as a result of the pandemic, but also because of the many new and emerging risks gaining attention over the last few years. We asked which new or emerging threats were causing the most concern.

Here is what we learned...

Seventy-four (74%) of survey respondents rated cybersecurity as a top concern.



This isn't surprising as there has been a constant stream of cyberattacks, data breaches and ransomware.

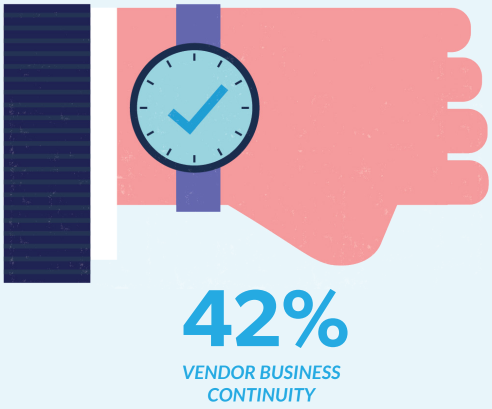
Examples are everywhere and there are many reasons to be concerned: the Colonial Pipeline ransomware attack, Facebook and LinkedIn data breaches and Microsoft Exchange's exploited vulnerabilities, to name a few. From a third-party risk perspective, there is no time for complacency.

Due diligence processes should be evaluated to ensure that vendors are held to the highest information security standards and organizations must remain vigilant for new cyber threats every day.

Copyright © 2022 Venminder, Inc

Fourth-party risk was also rated high (54%).

As an extension of your third-party risk, fourth parties can negatively impact your organization and customers. Require your third parties to disclose which of their vendors are considered critical and why. Hold your third parties accountable and ensure they have high standards for their own vendor management.

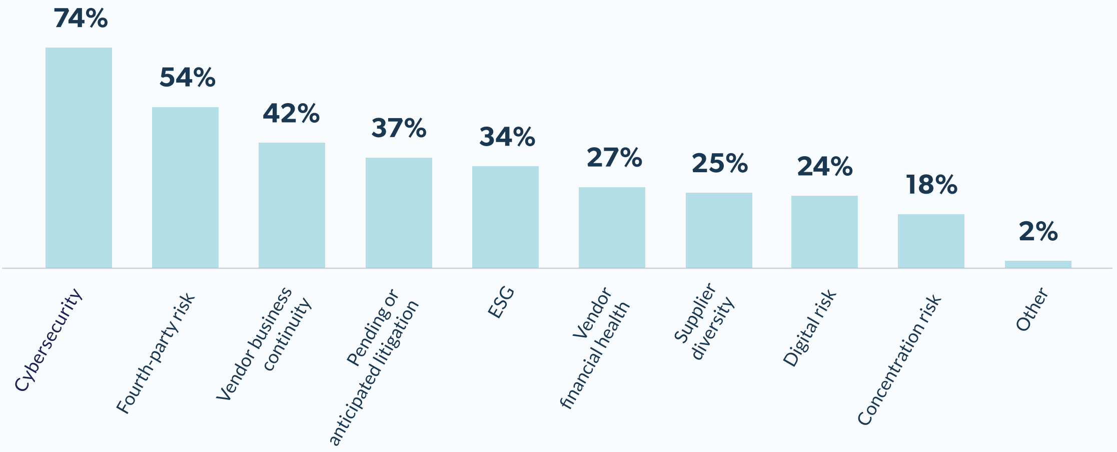


Vendor business continuity rounded out the top three at forty-two percent (42%).

Since the pandemic's beginning, many organizations have learned (sometimes the hard way) how important business continuity and recovery are. And there were plenty of reminders throughout 2021, such as the continuation of the pandemic and the winter storm in Texas. Vendors, especially those considered critical, need robust and tested business continuity plans.

Other emerging risks included ESG (34%) and vendor financial health (27%).

These were followed by supplier diversity (25%), digital risk (24%) and concentration risk (18%).



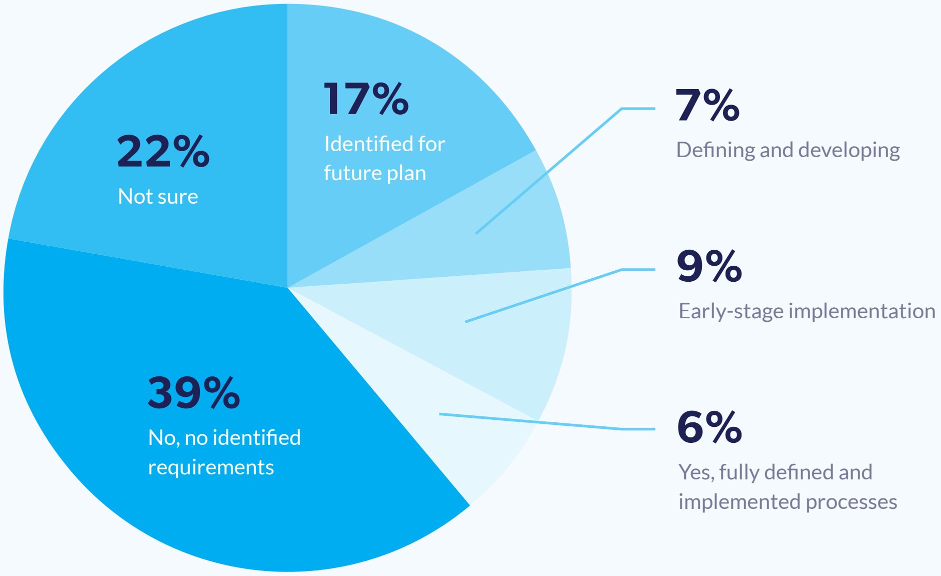
* Respondents were asked to mark all that applied

There has been a lot of discussion about environmental, social and governance (ESG) reporting and disclosure. However, in the U.S. there has yet to be any formal regulation or guidance to follow. Organizations serving foreign markets such as the EU and UK will be more familiar with ESG. Those countries lead many of the existing ESG efforts, though there are still fundamental questions about the actual ESG requirements for vendors.

Of the organizations with ESG in scope, only 6% have defined and implemented processes. Some are currently defining and developing their program (7%) or are in early-stage implementation (9%). Still, 61% of respondents have no requirements (39%) or are unsure (22%).

That 61% may benefit from an improved understanding of what ESG is and why transparency and reporting are essential, not just for regulators, but for investors and consumers as well. Remember, when the time comes to implement ESG into your TPRM program, it will require time and careful planning. ESG will become another risk type and due diligence component. Inherent risk and due diligence questionnaires need to be considered as does identifying the right subject matter expert to help you interpret and provide qualified opinions on ESG reporting.

Does your organization have an ESG (environmental, social and governance) disclosure and reporting requirement or process for your vendors?



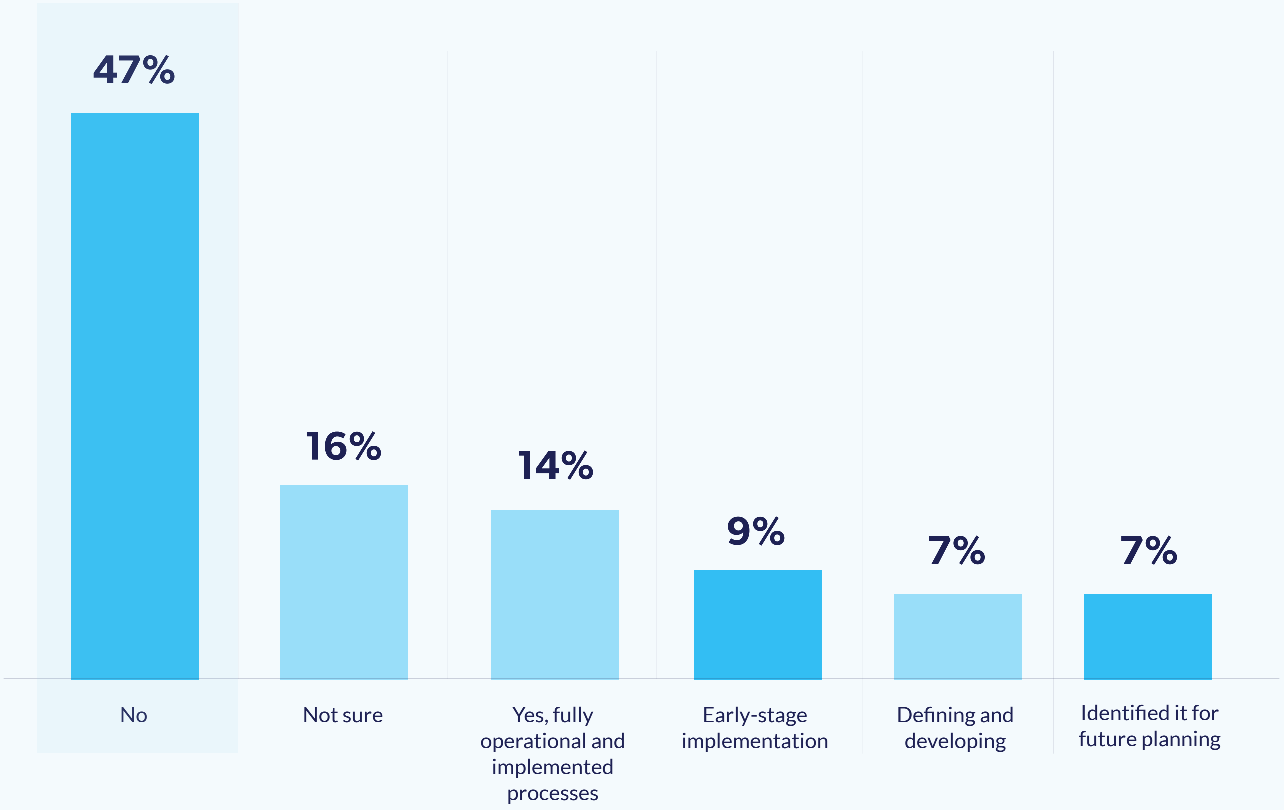
Copyright © 2022 Venminder, Inc

We were interested to find out how many of our survey respondents extended diversity and inclusion to include their vendors and collected this information as part of the vendor profile. 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.

Generally, capturing diversity as part of the vendor profile remains limited. In our survey, 47% of those responding didn't capture this data as part of the vendor profile and 16% were unsure.

Still, organizations are working towards this goal, as 7% had identified it for future planning. Another 7% are defining and developing the requirements and processes. Nine percent (9%) are in early-stage implementation. That leaves the 14% 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)?



Copyright © 2022 Venminder, Inc

Vendor Management Challenges

Not enough internal resources

This year, we had a tie for the number one issue. Not surprisingly, **"Having enough internal resources"** ranked first (40%), as did **"Getting the right documents from vendors"** (40%). These issues were rated first and second last year.

Getting the right documents from vendors	40%
Having enough internal resources	40%
Time management	27%
Automating the process	26%
Tailoring our due diligence requests to be appropriate for each vendor	23%
Completing risk assessments	20%
Keeping track of all the documents and data	17%
Managing contracts and negotiations	15%
Garnering senior management support	12%
Awareness of our vendor's cybersecurity	12%
Analyzing SOC reports	11%
Determining which vendors are critical to our organization	10%
Knowing who our vendors are	8%
Keeping up with the regulations	8%
Preparing for exams/audits	8%
Obtaining adequate budget	7%
Completing a financial analysis	6%
Other	6%
Reporting	5%
Keeping senior management informed	1%

***These results are based off respondents choosing their top 3 challenges**

Copyright © 2022 Venminder, Inc

So, the story hasn't changed; TPRM programs are still struggling. *Organizations are lacking dedicated full-time employees and funding for vendor management.*

Furthermore, there may not be enough credentialed and experienced professionals to get the job done effectively. TPRM programs are still searching for ways to better automate the process, tailor due diligence and get attention and support from senior leadership. Considering the increased internal and external pressures to improve vendor risk management, many organizations may be reaching a breaking point.

There are creative ways to address some of these challenges. For example, outsourcing processes like due diligence document collection and reviews can increase much needed bandwidth for internal TPRM teams and solve document collection issues. Another option is to utilize dedicated vendor risk management software to automate the process, improve efficiency and keep track of documentation.

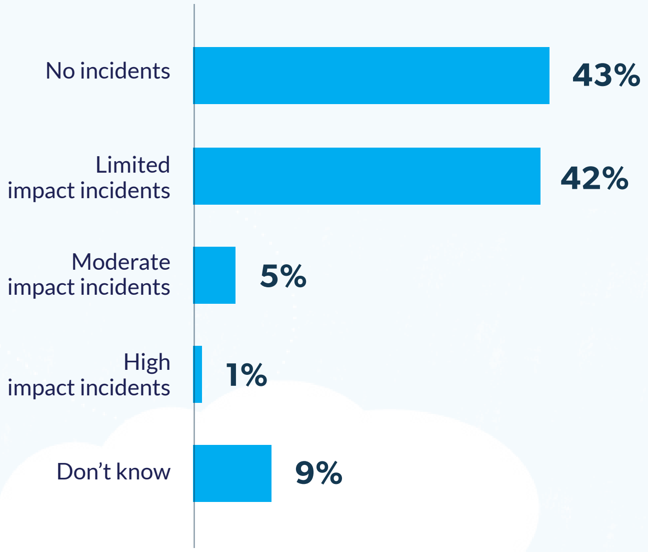
Copyright © 2022 Venminder, Inc

Pandemic Impact on Third-Party Risk Management

Things have definitely changed, yet the situation remains the same

During the second year of the pandemic, cyber incidents were still a regular occurrence, as nearly half of the respondents experienced a cybersecurity incident of some kind in 2021. Most of these were considered low impact. Moderate impact incidents increased only slightly as high impact incidents were reduced. Perhaps the lessons learned in 2020 helped keep the severity of these cyber incidents relatively low, and almost half of the respondents had no incidents.

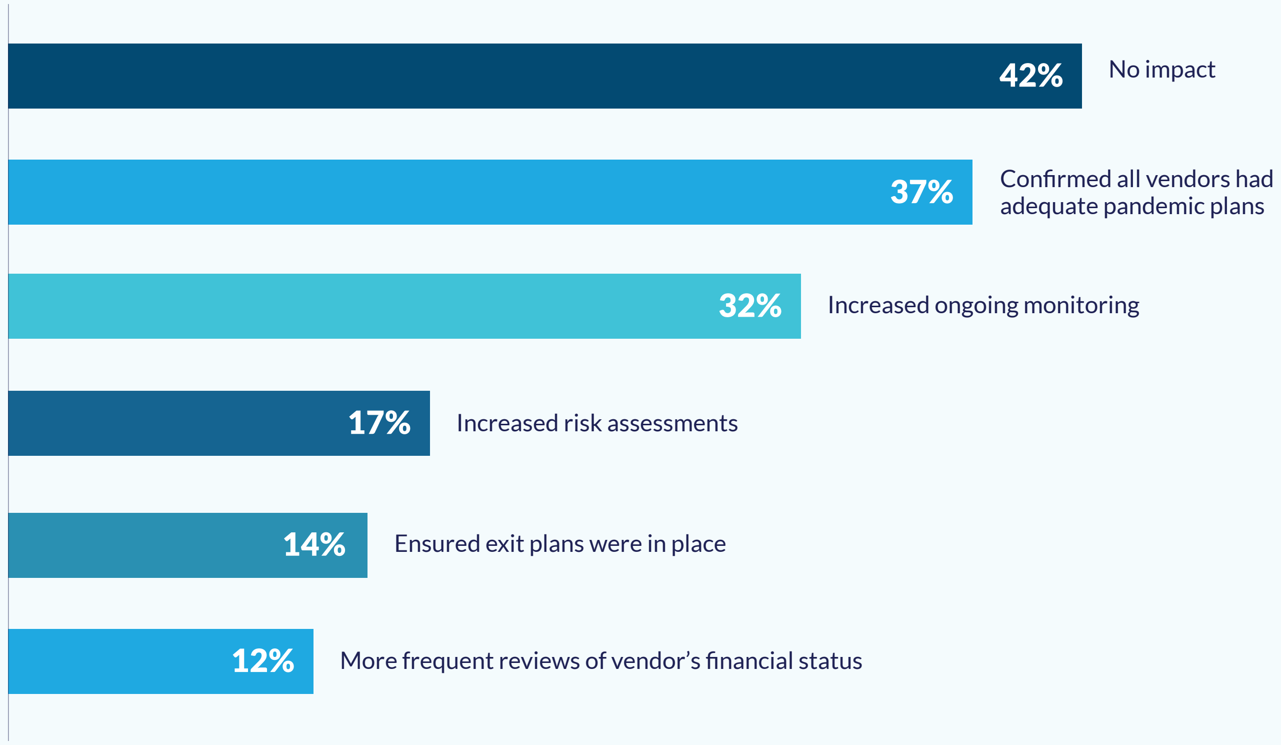
Did you experience third-party cyber incidents during 2021?



Compared to last year, TPRM programs were just a bit more relaxed when adjusting their processes because of the pandemic. This year many respondents replied that the ongoing pandemic had no real impact on their TPRM processes. We can guess this is because most of the heavy lifting happened in the previous year.

More participants are engaging in ongoing monitoring, which includes risk assessments and ensuring that exit plans are in place. This is encouraging as those are the measures to take now and make permanent for the future.

How has the COVID-19 pandemic impacted your third-party risk management processes?



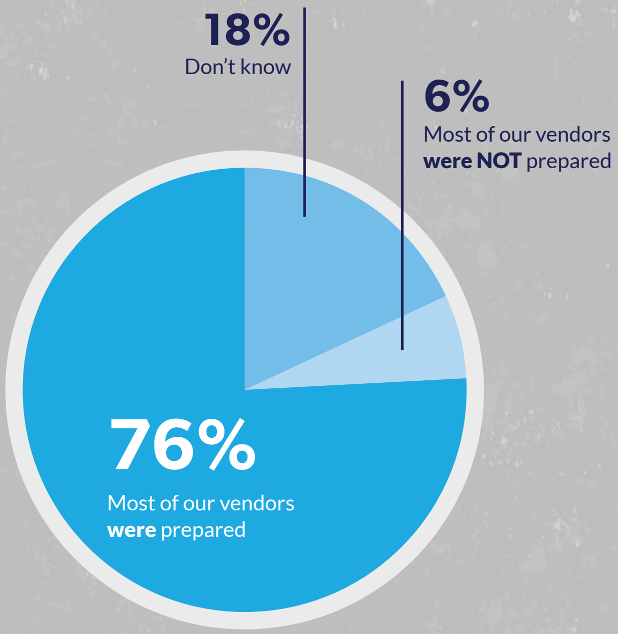
***Respondents were asked to mark all that applied**

In the first few months of the COVID-19 pandemic, **did your vendors have adequate pandemic plans in place to avoid impacting services to you/your customers?**

Copyright © 2022 Venminder, Inc

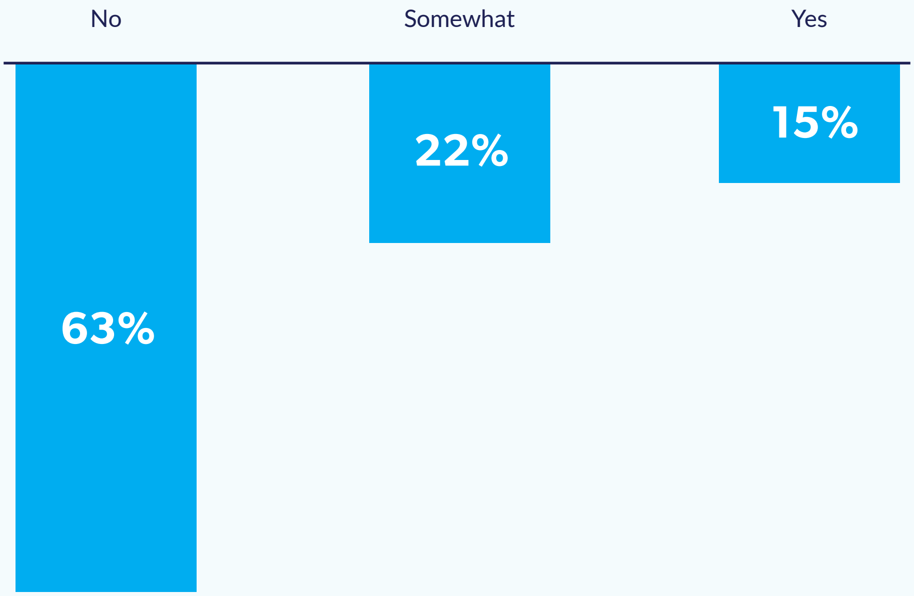
It seems that vendor business continuity planning has paid off. Seventy-six percent **(76%) of our survey sample said most of their vendors were prepared and implemented their pandemic plans with little or no impact on the organization.**

Throughout the COVID-19 pandemic, have your vendors had adequate pandemic plans in place to avoid impacting services to you/your customers?



Copyright © 2022 Venminder, Inc

Due to the pandemic, did your organization fall behind on core third-party risk management activities (such as annual risk assessments)?



In the earliest pandemic stages, organizations needed to reprioritize quickly to ensure their operations could continue. As time progressed and the dust settled, many organizations were met with the realization that “the show must go on” and that they had fallen behind on essential processes and needed to catch up. We asked if this was the case for our survey participants. As expected, 15% answered that they had fallen behind, and another 22% had fallen behind somewhat. It’s understandable under the circumstances that processes, such as annual risk assessments, had fallen behind. However, late risk assessments must be brought up to date as soon as possible, especially for critical vendors. One option for those who have fallen behind is to outsource risk assessments until everything is current or permanently outsource a portion of risk assessments to stay current.

> Keep in mind that each organization needs to make their own determination of risk level, even if assessments are outsourced.

Copyright © 2022 Venminder, Inc

Training and Education

For best results, offer the best training

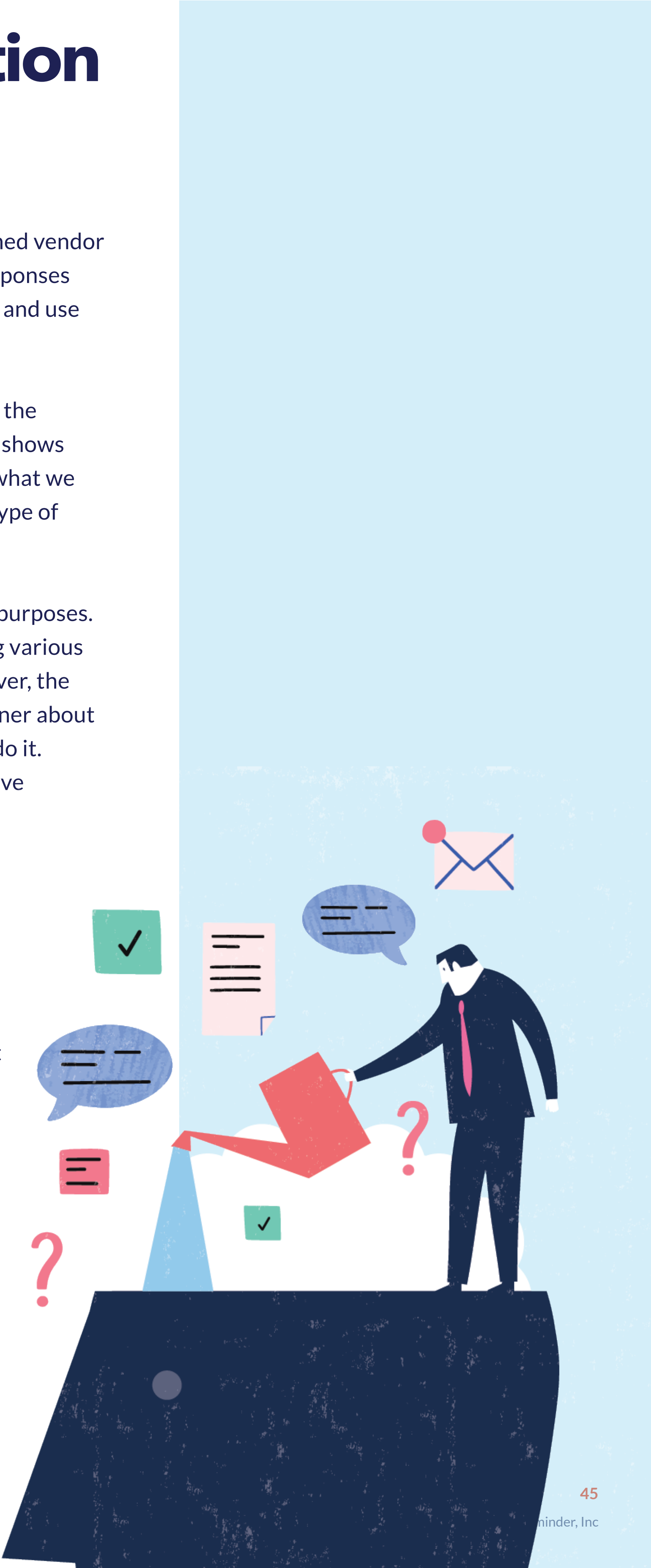
Our survey participants were asked if the organization trained vendor owners to perform vendor risk management duties. The responses revealed that most organizations train their vendor owners and use multiple formats to train them.

Personal instruction was a popular choice, as was providing the vendor owner with basic instructions and procedures. Roadshows and self-service online training are also utilized. Although, what we couldn't determine from this question was the quality and type of training content provided.

The truth is that vendor owner training serves two distinct purposes. The first is to provide practical instruction on accomplishing various vendor risk management tasks or the "how" we do it. However, the second, and less obvious, reason is to inform the vendor owner about the purpose and objectives of those tasks, or the "why" we do it. Often, training efforts are solely focused on the first objective without regard to the second.

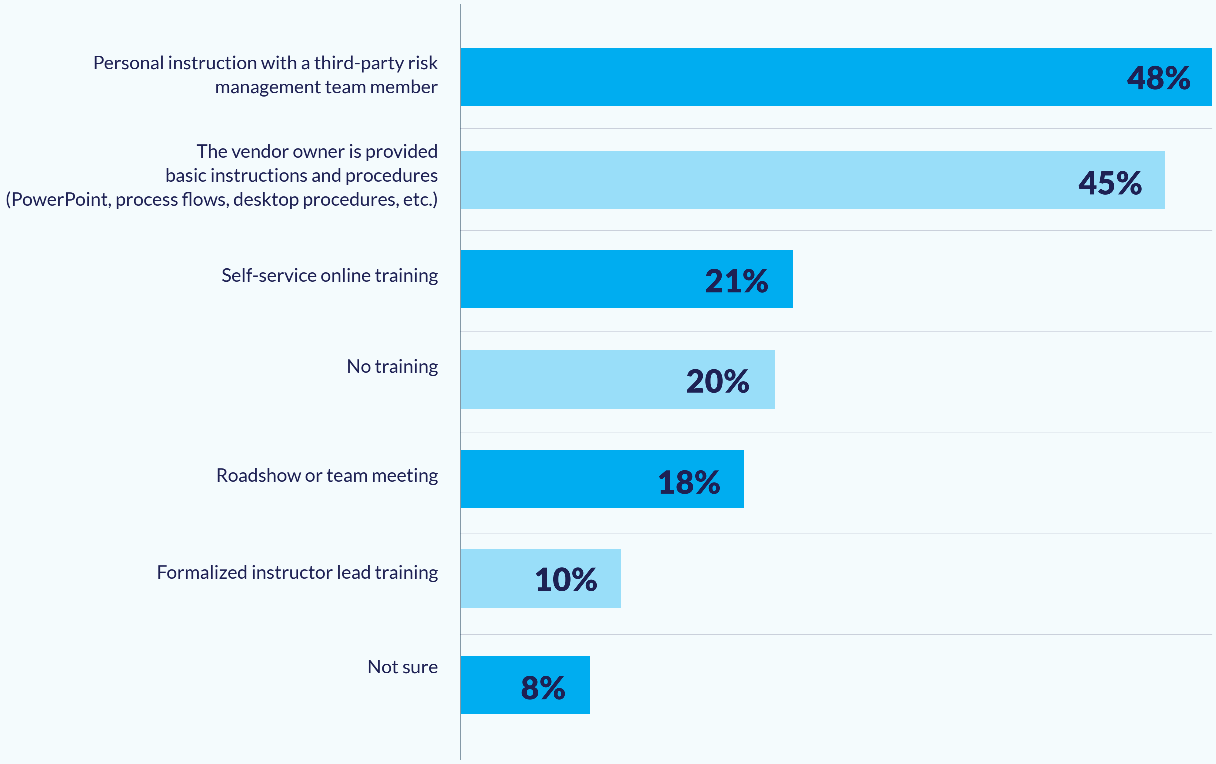
In an earlier survey question, we asked how difficult it was to secure buy-in or support from the line of business or vendor owner. Overwhelmingly respondents agreed it was either challenging or very challenging. In our experience, resistance often stems from a lack of confidence. Business owners with insufficient training may be less than confident about correctly fulfilling their third-party risk duties.

Even if they understand how to complete a task, it just becomes more work on their plate without understanding the real purpose of the task. This is why training is an essential part of successful vendor risk management programs.



minder, Inc

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



*** Respondents were asked to mark all that applied**

Good training teaches vendor owners how to complete their vendor risk management tasks. Great training reveals the real benefits of managing vendor risks. It also creates a sense of purpose and responsibility when fulfilling the vendor risk management function.

We encourage a review of vendor owner training materials to make sure they meet both the “how” and the “why” objectives, while also soliciting feedback on the training from the vendor owners. If you’re missing the “why,” you may have discovered one of the reasons getting that vendor owner buy-in has been so challenging.

Lack of resources is a real issue for most TPRM programs. Outsourcing parts of the TPRM process can be a viable solution to accomplish more while adding more bandwidth simultaneously.

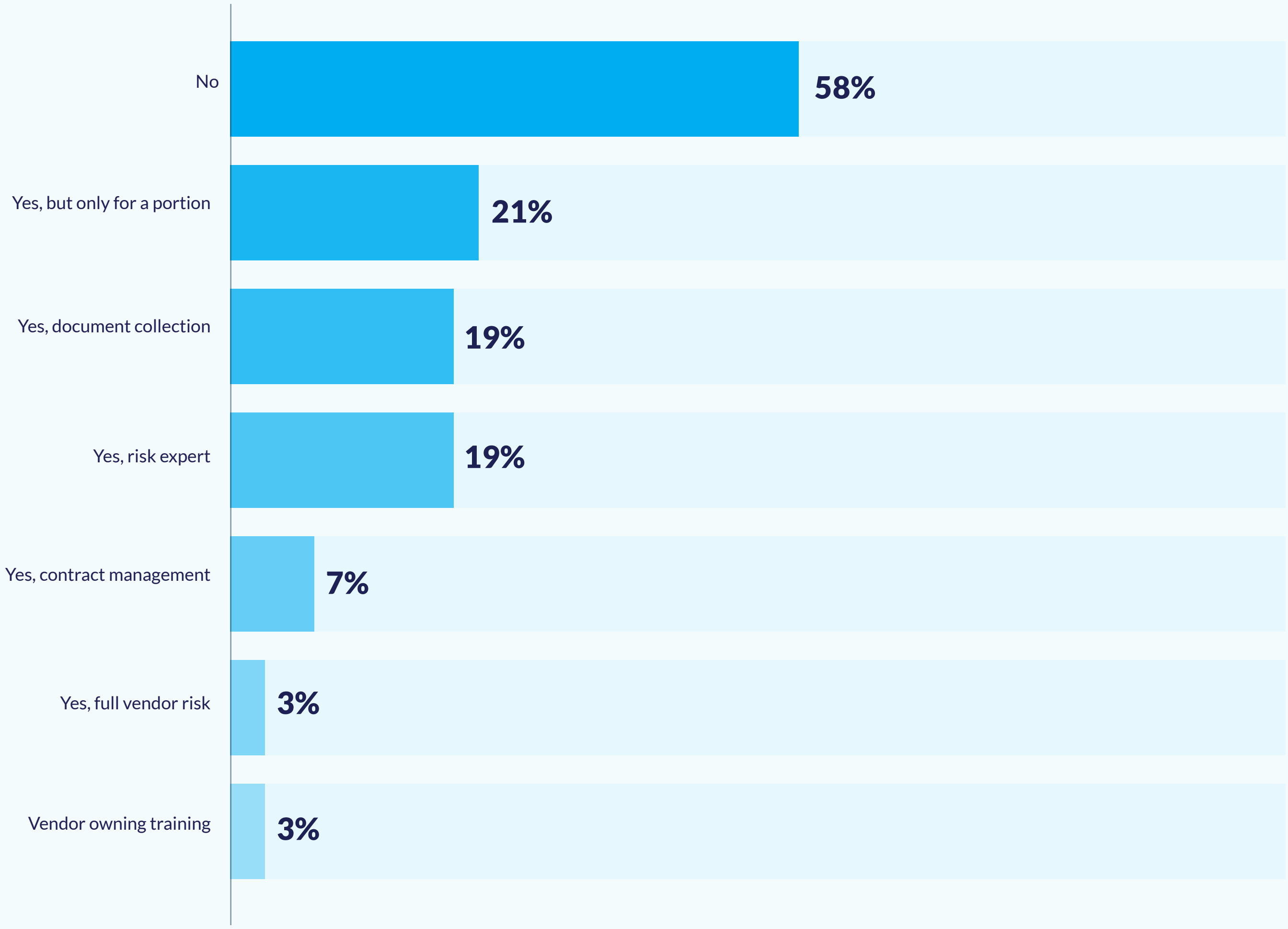
We wanted to see how many organizations were using outsourcing and what they were outsourcing.

Copyright © 2022 Venminder, Inc

As expected, a significant portion (58%) of respondents said they weren't using any outsourcing. For those who were, we found that 21% were only outsourcing a portion of the vendor portfolio. Other uses included risk expert reviews and due diligence document collection. A small portion (3%) was outsourcing their vendor owner training.

We predict that outsourcing will become a popular option to supplement in-house capabilities, especially since insufficient TPRM staffing is ongoing. However, we don't recommend outsourcing your entire vendor risk management program as 3% of our survey population is currently doing.

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**

Copyright © 2022 Venminder, Inc

ROI and Primary Benefits

Why we do what we do

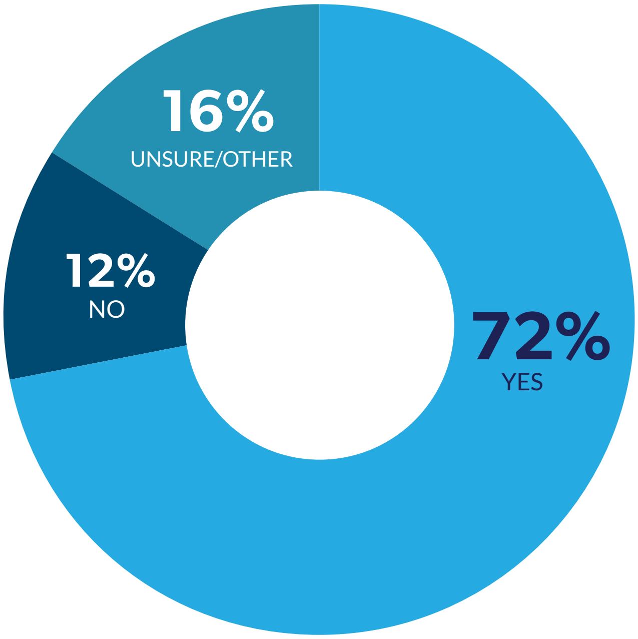
Successful TPRM enables better vendor selection, negotiation and cost savings. Furthermore, keeping track of vendor performance can lead to better or more meaningful service level agreements during contract renewal. It also provides necessary data points that can be used during contract renegotiation or when comparing multiple vendors.

Proactive third-party risk identification and effective risk management do as much for the bottom line as pure cost savings. Good TPRM often translates to cost avoidance and is realized through better management of contracts, improved third-party service levels, strong regulatory compliance and the prevention of business interruptions.

Effective TPRM also significantly reduces the possibility of litigation, regulatory fines, rework, lost productivity, reputational damage and negative impacts for your customers.

Seventy-two percent (72%) of our respondents agree that their organizations believe in a return on their TPRM investment. In comparison, only 12% didn't share that view and 16% were unsure.

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



Copyright © 2022 Venminder, Inc

Real Strategic Value

As they say, "an ounce of prevention is worth a pound of cure," and TPRM is all about risk prevention. Per the Ponemon Institute's 2021 Survey, the cost of a data breach is approximately $161.00 per customer record.

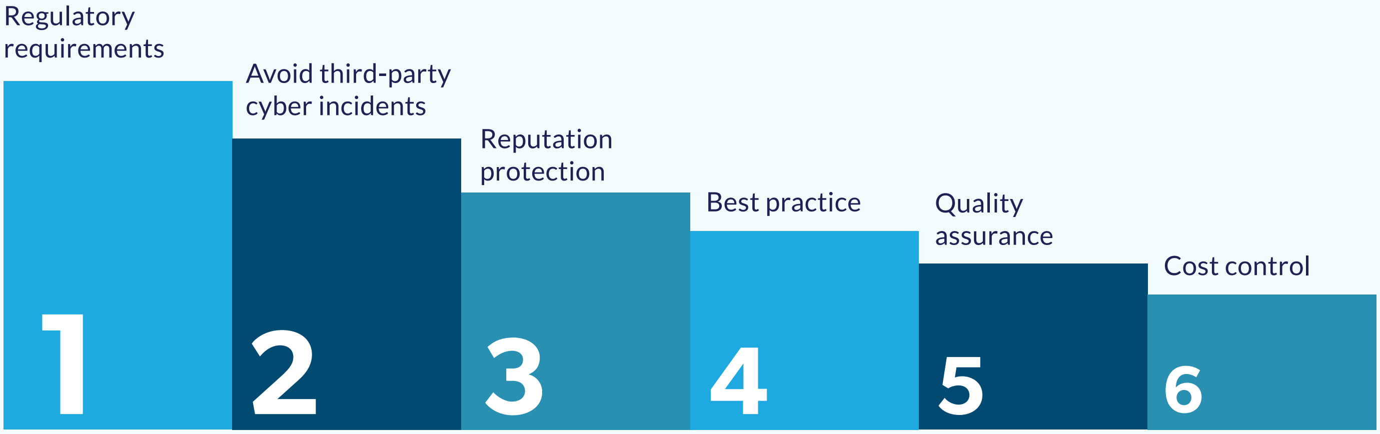
Calculate the possible expense to your organization using that figure, and the value proposition of TPRM becomes clear. Structured due diligence and ongoing risk monitoring help avoid costly data breaches, lost revenue, negative customer experiences and possible regulatory fines.

TIP

Suppose you're struggling to get finance or senior management to realize the value that TPRM brings to the organization. One way to get their attention is to add up all the costs of your contracts with third parties and calculate 2.5% of that total cost.

That figure represents the average of 2.5% of vendor expenses that's wasted every year on unintended auto-renewals.

Rank 1 to 6 your primary reasons for doing vendor risk management.



Vendor risk management as a practice lessens the potential for vendor-related incidents, including operational interruption, reputation damage and excess spending.

Unsurprisingly, regulatory compliance continues to be the number one reason organizations do vendor risk management. While meeting the regulators' expectations is a primary driver, compliance isn't the value of vendor risk management.

Copyright © 2022 Venminder, Inc

What do you believe the primary benefits vendor 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 vendor risk management. We've highlighted the answers below, removing duplicate answers.

It's clear that there are many benefits to vendor risk management.

Meets compliance and regulatory needs. It also informs internal experts on the latest security and data protection requirements.
Bank, $1B to $10B

Proper risk oversight to avoid costly losses and reputational bruises with a bad vendor.
Bank, $1B to $10B

Comfort over the controls and practices with 3P's to keep customer information confidential, processes and systems running.
Bank, $10B+

Reduces the likelihood of a third-party failure or incident which could affect customers, attract bad publicity and/or result in a fine from regulators.
Bank, $10B+

Security over controls and data access.
Information Technology & Services, 1,001-5,000 employees

Helps keep better track of expiration and auto **renew dates.**
Mortgage , 501-1,000 employees

Meeting regulatory and **client contractual requirements.**
Healthcare, 501-1,000 employees

Ensures a level of organization and due diligence in managing vendors. It's a one-stop area, as opposed to vendors being managed by separate departments.
Bank, $1B to $10B

Gives insight and confidence that **critical and material vendors are following or exceeding industry standards,** and maintaining a healthy all-around business practice. Additionally, if a vendor has questionable financials, SOC reports, security, etc., we can address those delinquencies with the vendor or vet a new vendor to maintain a strong relationship and safe business practices.
Credit Union, $1B to $10B

A review of a company is completed more often than if no vendor management policy was in place.
Mortgage, 1-100 employees

Helps manage information security risks, costs and tech time (e.g. the amount of work needed by tech to ensure our product performs as desired).
Fintech, 501-1,000 employees

Consistency and expertise.
Bank, $10B+

Provides another tool to build resilience.
Information Technology & Services, $1B to $10B

Copyright © 2022 Venminder, Inc

Helps identify **the extent of our reliance on third-party vendors.**
Credit Union, $1B to $10B

A safe and secure vendor program supports **business owner partnership**, cost control, adherence to regulatory requirements and risk-based processes.
Bank, $10B+

Mitigates business and regulatory risks.
Wealth/Asset Management, 1-100 employees

Avoids unanticipated risks. It also **supports consolidation** (leveraging existing relationships for greater discounts), cost reduction (deal renegotiations) and cost avoidance (unwanted renewals).
Fintech, 1,001-5,000 employees

Satisfies regulatory expectations.
Bank, $1B to $10B

Risk reduction.
Transportation, $10B+

Protects against reputational risk and **adheres to regulatory requirements**.
Financial Services, 5,001+ employees

Identifies risks to the organization; provides **clear oversight and reporting of vendor-related issues** to senior management; drives performance monitoring; and supports better contracts with vendors.
Holding Company, $10B+

With third-party risk-based management as core to our cybersecurity posture, **we benefit via DFS compliance and assurance that both shadow IT and IT-managed assets adhere to the same restrictions and policies to protect PHI, NPI and PII**. Third-party reviews also ensure that vendors are aligning to our cybersecurity program, contract, metrics and SLA objectives. Our business users are aware of and prepared to meet any cloud-based or third-party user entity controls to ensure the safety of our client's data, our business and the services providers we partner with.
Insurance, 101-250 employees

It forces the relationship **owner to evaluate the performance** of the third party in accordance to the agreement and cost/benefit.
Bank, Less than $1B

Mitigates the adverse impacts of a third-party risk event.
Wealth/Asset Management, 501-1,000 employees

Ensures that **risk assessments** are performed prior to signing contracts.
Insurance, 5,001+ employees

Provides control through managing expectations, vendor reviews, software reviews and cybersecurity reviews. It stops the willy-nilly people who are full of self entitlement and think they can do whatever/whenever/however.
Fintech, 1-100 employees

Compliance and **external** audit success.
Healthcare, 501-1,000 employees

Gives information on potential risks based on events happening at our supplier, supplier location or country.
Mechanical or Industrial Engineering, $1B to $10B

Risk management of third parties.
Lender, 251-500 employees

Cost savings, **better contract negotiation** and business continuity.
Wealth/Asset Management, 1,001-5,000 employees

Another set of eyes.
Bank, Less than $1B

Copyright © 2022 Venminder, Inc

It keeps the banks safe and education is important to keep us informed of what's going on in the world.
Bank, $1B to $10B

Gives us knowledge into our third parties' practices, security and financial health.
Credit Union, Less than $1B

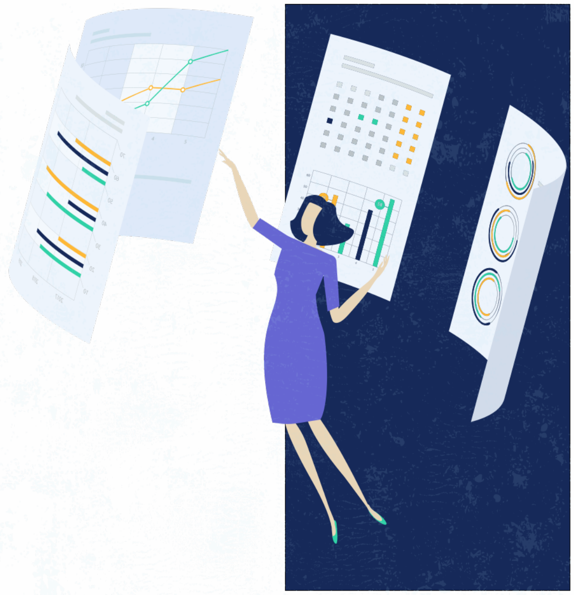
Identifies potential reputational risks before they occur, monitors and collects information about client data protection, and demonstrates a comprehensive vendor program for regulators.
Financial Services, 101-250 employees

Makes our examiners happy.
Credit Union, Less than $1B

Gives **greater visibility into vendor risk** and risk avoidance.
Insurance, 5,001+ employees

Compliance.
Information Technology & Services, 1,001-5,000 employees

Knowledge of industry trends and risk threats.
Bank, Less than $1B



Adheres to regulatory requirements, **provides safety for third-party engagements** and assures of operating controls at third party.
Bank, $10B+

Auditor compliance.
Credit Union, Less than $1B

More leverage on the third party's resources.
Package/Freight Delivery, $10B+

Provides a better understanding of the required **risk management mitigations**.
Tobacco, $10B+

Ensures thorough due diligence before selecting a third-party vendor partner and provides **consistency with managing contract renewals** before they rollover or expire because dates weren't tracked correctly.
Bank, $1B to $10B

Manages risk - regulatory, financial, operational, etc.
Bank, $10B+

Helps **identify which vendors are most vulnerable.**
Credit Union, $1B to $10B

Mitigates risk, provides visibility to management and **better security/protection**.
Insurance, 251-500 employees

Avoids business losses and interruptions and protects reputation.
Healthcare, 251-500 employees

Provides proactive planning, assists in obtaining value for money, reduces organization's exposure to disruptive events, reputation protection.
Credit Union, $1B to $10B

Provides reminders for documentation reviews of SOC, contracts, disaster recovery, cyber, financials, etc.
Credit Union, Less than $1B

Ensures overall risk can be identified.
Bank, $1B to $10B

Copyright © 2022 Venminder, Inc

Gives us a **timely review of contracts** (sufficient time to negotiate costs and/or services). It also reduces time spent by staff in the vendor management process, thus freeing up time to spend on other projects/ assignments.
Credit Union, Less than $1B

Provides oversight of the financial and technological capabilities of the third party.
Credit Union, $1B to $10B

Arms vendor relationship **owners with some tools to better manage** and assess the risk of their vendors. Gives vendor relationship owners some leverage with their vendors and allows them to ask more from their vendors.
Credit Union, $1B to $10B

Satisfies the regulatory requirements.
Bank, $1B to $10B

Regulatory compliance, **reduced vendor risk.**
Bank, $1B to $10B

Helps **protect our cyber environment.**
Healthcare, 101-250 employees

Ensures **client confidence** and risk mitigation.
Wealth/Asset Management, 501-1,000 employees

Gives us **additional compliance** support.
Bank, $10B+

Keeps our **customers safe.**
Bank, $1B to $10B

Mitigates severe impacts to employees, revenue and reputation.
Retail, 5,001+ employees

Provides risk awareness that allows for educated decision-making. It reduces third-party risk due to control **awareness and gives us the ability to react quicker** to third party-related events by knowing who our third parties are.
Bank, $10B+

Provides **visibility into third parties** and the risks they pose. It also supports compliance.
Bank, $1B to $10B

Gives **peace of mind** and complies with regulations.
Bank, $10B+

It enables our company to be **better equipped to handle/ predict** any third-party related events.
Bank, $1B to $10B

Protects our customers' confidential information and **provides the safest third-party solutions for the bank and our customers**. Gives us insight into our vendors' strengths and weaknesses, allowing us to choose the best products. Knowing those strengths and weaknesses allows us to formulate better risk mitigation strategies.
Bank, $1B to $10B

Risk control.
Bank, $10B+

Regulatory relief.
Bank, Less than $1B

Provides security in auditing and meeting compliance.
Defense & Space, $10B+

Lessens the time **dealing with bad invoices** and failing suppliers.
Information Technology & Services, 1-100 employees

Protects data privacy and security and supports regulatory compliance.
Leisure, Travel & Tourism, Less than $1B

Helps us stay organized and gives us time for other things.
Bank, $1B to $10B

Satisfies **auditors and regulatory** compliance.
Healthcare, 251-500 employees

Mitigates risk to the bank and supports contract management.
Bank, $1B to $10B

Copyright © 2022 Venminder, Inc

It helps internal stakeholders rest easier. But I believe the true value of third-party risk management exists when multiple entities subject vendors to it. It sets expectations for vendors to meet, and pushes them to take reasonable steps to mitigate their risks.
Bank, $1B to $10B

Helps exponentially when it comes to audit time and meeting our regulatory standards. We have prevented several questionable vendors from being purchased, thereby protecting our proprietary as well as our member's data. We maintain vendor lists so if there's an information security breach at one of the big suppliers (i.e. SolarWinds, Kaseya, etc.), we're able to mobilize and make contact with our other vendors who may use them too.
Credit Union, $1B to $10B

Risk aversion.
Credit Union, Less than $1B

Gives confidence that we aren't missing compliance dates and that we are compliant to regulators.
Mortgage, 101-250 employees

Reduces contract risk and **centralizes information**.
Bank, $10B+

Secure and effective outsourcing.
Information Technology & Services, 251-500 employees

Regulatory compliance.
Credit Union, $1B to $10B

Security.
Credit Union, $10B+

Helps avoid financial loss, project delays and reputation damage.
Healthcare, 501-1,000 employees

Consolidates list of active vendors. **Provides knowledge of the risks associated with each vendor**. And having an effective program keeps regulators out of our hair.
Insurance, 501-1,000 employees

Provides sound risk mitigation practices and adequate evidence to satisfy regulators.
Bank, $1B to $10B

Satisfies regulatory requirements.
Mortgage, 251-500 employees

Fosters better partnerships between the risk management division and other divisions within the bank.
Bank, $10B+

Regulatory compliance.
Bank, Less than $1B

Provides **assurance of data protection throughout the supply** chain and visibility of critical vendors. It helps with vendor consolidation/reduction, risk mitigation and reduction.
Information Technology & Services, 1,001-5,000 employees

Risk management.
Bank, $1B to $10B

Maintains compliance with laws and regulations. Also **maintains controls to reduce reputation and operational risk**.
Bank, Less than $1B

Helps us to be efficient in **contract management and reduce our risk.** Also helps control damage to the bottom line.
Credit Union, Less than $1B

Gives proper insight into third-party risks.
Bank, $10B+

Risk management of third parties.
Bank, $1B to $10B

Compliance.
Bank, $1B to $10B

Enables better and stronger award decisions.
Consulting, 101-250 employees

We have **greater clarity and insight into the health and risks of our third-party partners**. It allows us to plan for and mitigate any risks and to monitor third-party performance relative to contracts.
Bank, Less than $1B

Copyright © 2022 Venminder, Inc

Reduces our risk and meets the regulatory requirements.
Credit Union, $1B to $10B

We are better **organized to implement change.**
Credit Union, $1B to $10B

Gives us good oversight of **where funds are being allocated** for each department.
Credit Union, Less than $1B

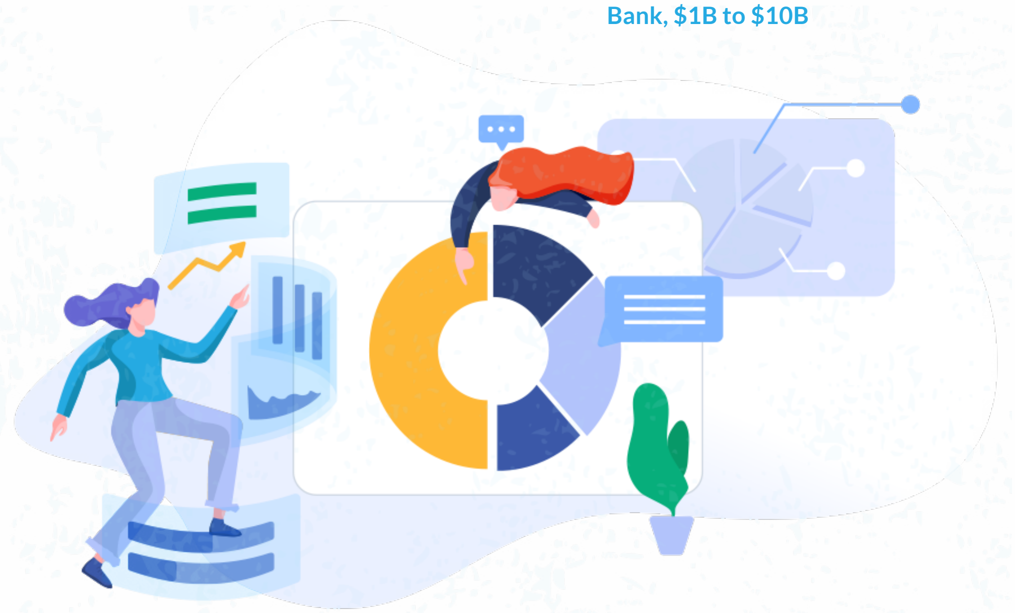
Assesses vendor criticality.
Bank, Less than $1B

We can **understand and align vendor risks** with our overall risk profile.
Bank, $10B+

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

Compliance.
Healthcare, 5,001+ employees

Contract management.
Credit Union, $1B to $10B



Meets regulatory requirements. It provides the value of vetting/monitoring vendors, centralized contract management, risk assessments and a due diligence system.
Bank, $1B to $10B

Gives us **cost-savings initiatives via procurement** and reduces risks that result from audit findings.
Mortgage, 5,001+ employees

Ascertains risks and potential mitigation involving vendors.
Bank, Less than $1B

It's an early warning **indicator of financial trouble** at critical vendors.
Credit Union, Less than $1B

Security.
Bank, $10B+

Avoids fraud and reputation risks.
Lender, 501-1,000 employees

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

It provides an **annual review of the vendor's health**. Contract negotiation is based on performance and it sets the tone for how much your vendor is willing to help you.
Credit Union, $1B to $10B

Enables us to respond to our client's due diligence questions related to the vendors we use. It verifies that our vendors have **the proper information security controls**, business continuity controls, operational controls and/or data privacy programs in place to protect us and are readily available.
Wealth/Asset Management, 251-500 employees

Due diligence.
Entertainment, Less than $1B

Transparency with vendors.
Bank, $1B to $10B

Gives advice and support to diversified procurement operations. **Reduces and mitigates risk**.
Bank, $10B+

Predicts future concerns.
Bank, $1B to $10B

We can **know our vendors.**
Bank, $1B to $10B

It can potentially **identify risks prior** to events.
Insurance, 501-1,000 employees

Copyright © 2022 Venminder, Inc

Ensures we have a program in place to **consistently address third-party risk** to the company as it relates to cybersecurity, BC/DR and privacy to meet regulatory requirements.
Insurance, 501-1,000 employees

Identifies, evaluates, monitors and manages potential threats/risks that stem from the use of our vendors and affiliates. **Gives insight into fourth parties.**
Fintech, 1,001-5,000 employees

Keeps us up to date on all documents needed to **assure the credit union that the vendor is in good standing**.
Bank, Less than $1B

Mitigates risk, provides risk awareness and improves vendor performance.
Healthcare, 5,001+ employees

Organization.
Bank, $1B to $10B

We believe strong **TPRM creates efficiencies, leading to cost savings** and time savings, while reducing compliance and reputation risk.
Credit Union, Less than $1B

Keeps us organized.
Credit Union, $1B to $10B

Improves safety and leads to cost savings.
Healthcare, 251-500 employees

We can **organize more** with less labor input.
Information Technology & Services, Less than $1B

Provides a **comfortable level of risk.**
Wealth/Asset Management, 1-100 employees

Complies with regulations and manages risk. Provides cost savings in vendor contracts and ensures contractual standards. It gives us an inventory of third parties and a centralized location for contracts.
Insurance, 251-500 employees

Complies with laws and regulations. **Protects our business** and customers.
Bank, $1B to $10B

Provides risk mitigation, organization and compliance.
Insurance, 1-100 employees

Gives us **information security comfort** and mitigates risk.
Insurance, 1,001-5,000 employees

Compliance.
Bank, $1B to $10B

Oversight.
Bank, $10B+

There are unrealized benefits and potential, such as the selection, procurement and maintenance of a vendor that could be more beneficial to the organization than other contenders. This could relate to compliance requirements, contracts, the relationship, regulations, etc.
Bank, $1B to $10B

Security.
Credit Union, $1B to $10B

Customer service and security.
Information Technology & Services, $10B+

Ensures the **confidentiality, integrity and availability** of customer data and bank information is protected.
Bank, $10B+

Gives us the **ability to focus** on vendor issues.
Bank, Less than $1B

Supports cost savings, regulatory compliance and **risk awareness across business units**.
Credit Union, $10B+

Mitigates risk and complies with regulations.
Bank, $10B+

Ensures data security, ensures regulatory compliance, reduces expense, and minimizes reputation risk.
Credit Union, $1B to $10B

Consistency and efficiency.
Credit Union, $1B to $10B

Copyright © 2022 Venminder, Inc

Provides knowledge of risks posed by third parties and **ensures the controls are in place** to mitigate those risks.
Wealth/Asset Management, 101-250 employees

It enables us to minimize the risks to our business resulting from an issue caused by the performance/activity of a third party.
Fintech, 1,001-5,000 employees

Completes the picture of the enterprise-wide risk profile in order for senior management to make proper decisions.
Mortgage, 5,001+ employees

TPRM helps us to **better understand the risks that utilizing our vendors can pose**, enables us to find ways to mitigate those risks and to make sound decisions when choosing vendors, and ensures that they can support us both operationally and financially.
Bank, Less than $1B

Risk reduction.
Bank, $10B+

Protects against breaks in supply chain.
Information Technology & Services, 1-100 employees

Mitigates **financial, reputational and security risks.**
Information Technology & Services, 5,001+ employees

Accountability.
Fintech, 1,001-5,000 employees

Monitors critical and high-risk vendors. Supports contract review and the appropriate onboarding process.
Wealth/Asset Management, 251-500 employees

It lessens regulatory scrutiny and provides **better data/ information security protection**.
Bank, Less than $1B

Gives us **regulatory compliance assurance** and mitigates risk.
Healthcare, 501-1,000 employees

Provides insight into a **vendor's security posture.**
Automotive, $10B+

Risk reduction.
Wealth/Asset Management, 101-250 employees

Avoids regulatory impact.
Fintech, 501-1,000 employees

Ensures compliance with regulations. **Enhances client experience** and mitigates against strategic and operational risks.
Wealth/Asset Management, 1-100 employees

Protects against **reputational risk and loss of member** information.
Credit Union, Less than $1B

Reduces operational and reputational risk to our organization.
Insurance, 5,001+ employees

Supports operational and financial efficiencies. Verifies the security of our vendor supply chain.
Bank, Less than $1B

Offers better data and consistent processes across the organization. Gives us more reporting and dashboards for snapshots and details of our vendors' risks.
Insurance, 501-1,000 employees

It's a **best practice**.
Information Technology & Services, 1-100 employees

Gives us greater insight into who has **access to our data** and where it is being housed.
Information Technology & Services, 5,001+ employees

Copyright © 2022 Venminder, Inc

It's **another vantage point** for evaluating risk.
Education, 501-1,000 employees

Provides risk mitigation, **compliance and value**.
Bank, $1B to $10B

Provides **risk management, portfolio rationalization**, supply chain threat management and process management.
Information Technology & Services, 1,001-5,000 employees

Gives us cost savings, efficiency, control, business continuity and risk management.
Healthcare, 1,001-5,000 employees

Reduces risk and manages vendors. It also provides cost savings.
Government, 1,001-5,000 employees

Gives us data security and financial savings through negotiations and reputation protection.
Insurance, 501-1,000 employees

Delivers consistent policy, training and **framework for onboarding**. Monitors and effectively manages third parties.
Bank, $10B+

Gives us protection and trust.
Telecommunications, 5,001+ employees

Gives us the ability to review new vendors to ensure they meet our privacy and security policies prior to procurement. **Meets compliance requirements** for annual reviews of high-risk vendors.
Information Technology & Services, 1,001-5,000 employees

Offers risk avoidance as well as **cost optimization**.
Bank, $10B+

Due diligence.
Credit Union, Less than $1B

Reduces risk of heavy tech outsourcing.
Bank, Less than $1B

Risk awareness.
Bank, $10B+

Centralizes knowledge of all the third parties we use and their services or products. Evaluates the risks associated with each third party.
Insurance, 501-1,000

Forces the relationship **owner to evaluate the performance** of the third party in accordance to the agreement and cost/benefit.
Bank, Less than $1B

Reduces the risk of third-party suppliers to acceptable levels.
Information Technology & Services, 5,001+ employees

Ensures **risk assessments** are performed prior to signing contracts.
Insurance, 5,001+ employees

We assess for cyber risk.
Construction, 5,000+ employees

Supports **regulatory compliance** and gives information security access to vendor controls.
Credit Union, $1B to $10B

Adheres to regulatory and compliance requirements.
Fintech, 5,001+ employees

Automation.
Credit Union, Less than $1B

Copyright © 2022 Venminder, Inc

Avoids regulatory sanctions, client disatisfaction and GSE scrutiny.
Mortgage, 1,001-5,000 employees

Maintains regulatory and **operational compliance.**
Fintech, 1-100 employees

Improves supply-chain security and protection of sensitive data.
Information Technology & Services, $1B to $10B

Mitigates **regulatory, reputational, cybersecurity and information security risk**. Lessens the initial financial investment.
Insurance, 1,001-5,000 employees

Provides data security and **protects against regulatory sanctions**. Presents M&A opportunities.
Bank, $10B+

Safety and security.
Mortgage, 1,001-5,000 employees

Achieves the **strategic objectives** of our organization.
Insurance, 1,001-5,000 employees

Supports business **resilience and reputation** protection.
Insurance, 5,001+ employees

Provides insight into the level of risk the organization is assuming.
Insurance, 1,001-5,000 employees

Protects the organization on so many different levels.
Bank, $10B+

Reduces risk and provides cost savings.
Insurance, 101-250 employees

Mitigates risk, helps us **find the best and most innovative vendors** and aligns with industry best practices.
Fintech, 1,001-5,000 employees

Better compliance.
Brokerage, 5,001+ employees

Provides clear guidelines on what is to be expected from client/vendor relationship. Analyzing risk assessment provides an in-depth detail while **protecting our organization from a variety of threats**.
Credit Union, Less than $1B

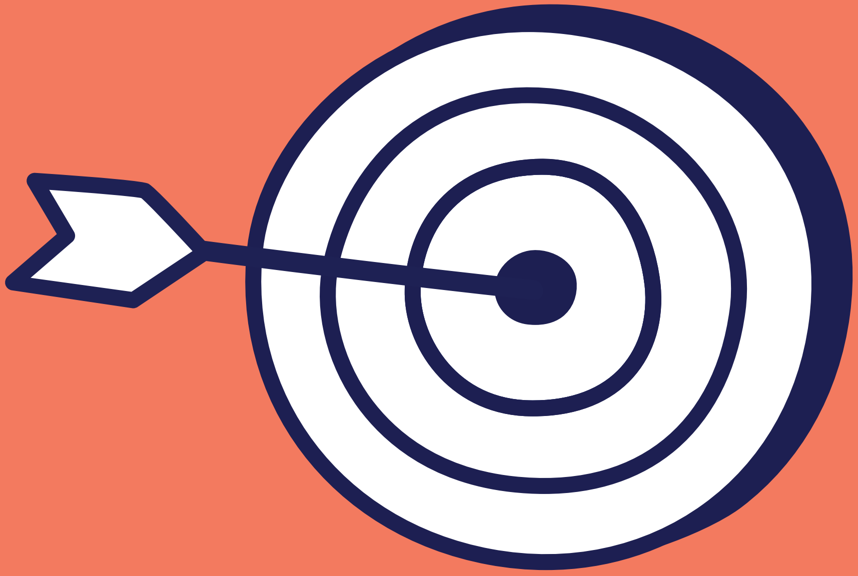
Offers a **consistent approach** across the organization to identify, monitor and assess risk.
Insurance, 5,001+ employees

Helps maintain **better, more efficient operations** and improves spend management. Provides market insights on trends.
Bank, $1B to $10B

Results in **clean audits** and exams.
Information Technology & Services, 251-500 employees

Copyright © 2022 Venminder, Inc

Recommendations & Best Practices



Copyright © 2022 Venminder, Inc

Insights from working with thousands of clients

The past couple of years have put many organizations' vendor risk management processes to the test. It was a good time to learn not only from the challenges we faced ourselves, but also from the experiences of others. Keeping informed and understanding what our industry is experiencing is a good indicator of where the third-party risk management road may lead.

Good news is it's a new year for all. Where your vendor risk practices need a checkup, now is the time. There are some best practices – old and new – that will help all industries improve their vendor management posture:

Best Practices for 2022

1. **Continue to invest and track** the investment of time and resources
2. **Have well-documented governance documents** such as a policy, program and set of procedures
3. **Use lessons learned in the pandemic** to determine what went well and what to improve
4. Ensure adequate and appropriately **experienced staffing**
5. **Educate** all levels of management and anyone who works with vendors
6. Keep documents and due diligence artifacts **up to date and relevant**
7. Stay on top of the **industry news and enforcement actions**
8. Monitor and track **vendor issues through remediation**
9. Keep senior management **well informed**
10. **Measure the impact** of vendor management and make sure practices are consistent with the enterprise risk management program

Copyright © 2022 Venminder, Inc

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 1000 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

Copyright © 2022 Venminder, Inc

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.

Copyright © 2022 Venminder, Inc.