State of Third-Party Risk Management

2021

venminder

Table of Contents

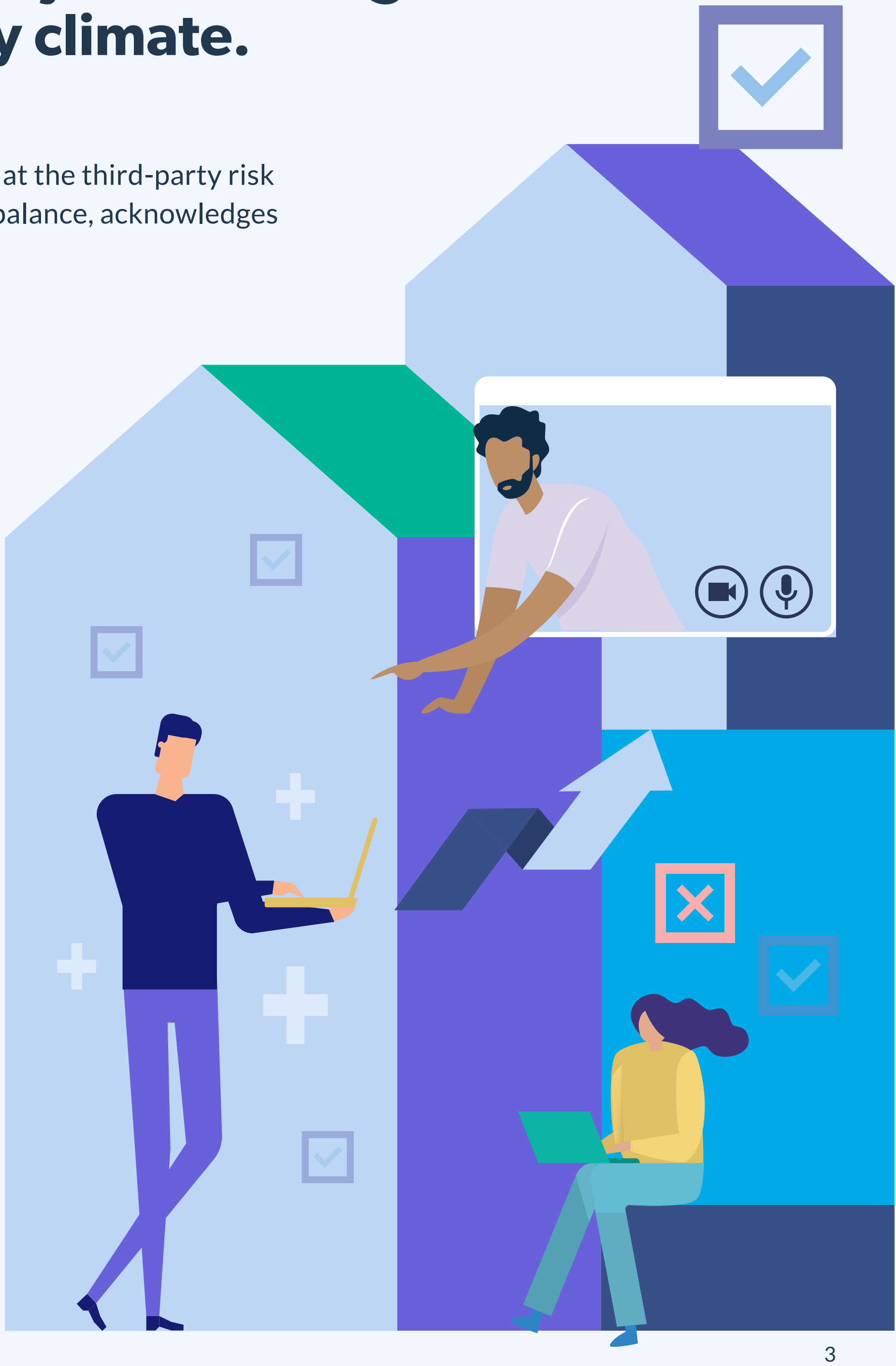
Executive Summary

Venminder's State of Third-Party Risk Management 2021 survey provides insight into how organizations are managing third-party risk management in today's increasing regulatory and risky climate.

The results provide a broader lens to look at the third-party risk management industry as a whole and, on balance, acknowledges the shared challenges.

This is Venminder's fifth annual whitepaper to survey individuals from a wide variety of organizations and industries including financial services, non-bank lending, mortgage, financial technology, insurance and more. In light of the ongoing pandemic, we also added in specific questions to understand how respondents' third-party risk management programs were impacted.

Venminder promoted the survey publicly through email, social media and the Third-Party ThinkTank online community during December 2020 and January 2021. To increase confidence in the validity of responses, answers were anonymous and confidential.



As 2020 brought about unprecedented change, it's particularly relevant that we look for shared lessons learned, best practices to follow, challenges faced and ways to continuously improve our third-party risk management practices.

Third-party risk management was very much tested as an operational risk mandate, rather than simply a regulatory requirement in 2020. The pandemic pushed organizations to be more innovative, work remotely and rely more heavily on outsourced practices. The (still ongoing) COVID-19 pandemic has validated for many that third-party risk management isn't just a regulatory issue, but a practical real-world consideration. It has driven heightened awareness in the need for well-managed third-party risk management practices and the importance in ensuring that your data is protected, whether it's in your hands or a vendors, and wherever it is – whether in a remote or office environment.

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 third-party risk management.

Survey Highlights

Venminder's State of Third-Party Risk Management 2021 Survey provides insights that allow for peer-to-peer learning and the ability to benchmark against current best practices.

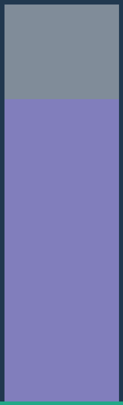
Here are just a few survey highlights:

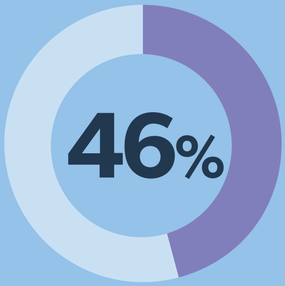
The maturity of third-party risk management practices continues to **evolve and, notably, improve**

More organizations than ever are placing a **priority on third-party risk management**, as evidenced by the budget investment of budget expenses increasing for many

76%

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





46%

have **between 1 and 2 employees dedicated to third-party risk management**

Organizations are continuing to see a practical advantage of third-party risk management as a **positive return on investment (ROI)**

The #1 biggest vendor management challenge is **not having enough internal resources to manage the workload**

Survey **Results**

Commitment to Vendor Management

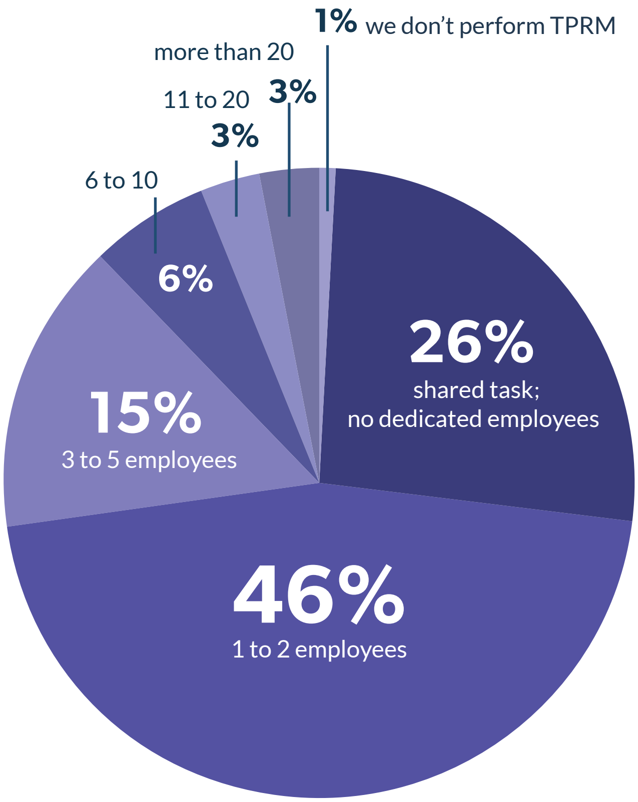
Internal Resources Committed to Vendor Management

Real concerns in certain areas

Twenty-six percent (26%) of organizations report having no employees dedicated to vendor management and instead rely on existing employees to share the workload of this crucial function. It's encouraging that today, 73% of organizations have dedicated employees to run their vendor management programs, with 46% having between 1 and 2 employees, 15% having between 3 and 5 employees, 6% having between 6 and 10 employees and 6% having more than 6 employees.

It's important that management today are aware of the vital role that third-party risk management plays in the organization. Seeing that almost 75% of our sample base had less than two people dedicated to third-party risk management tells us that the constraints on people's time will continue to be tested as the associated workload is not small. Having a properly staffed organization, including properly experienced and credentialed personnel, is key to establishing practices that are not only compliant with regulatory guidance, but also truly serves the organization in mitigating risk.

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



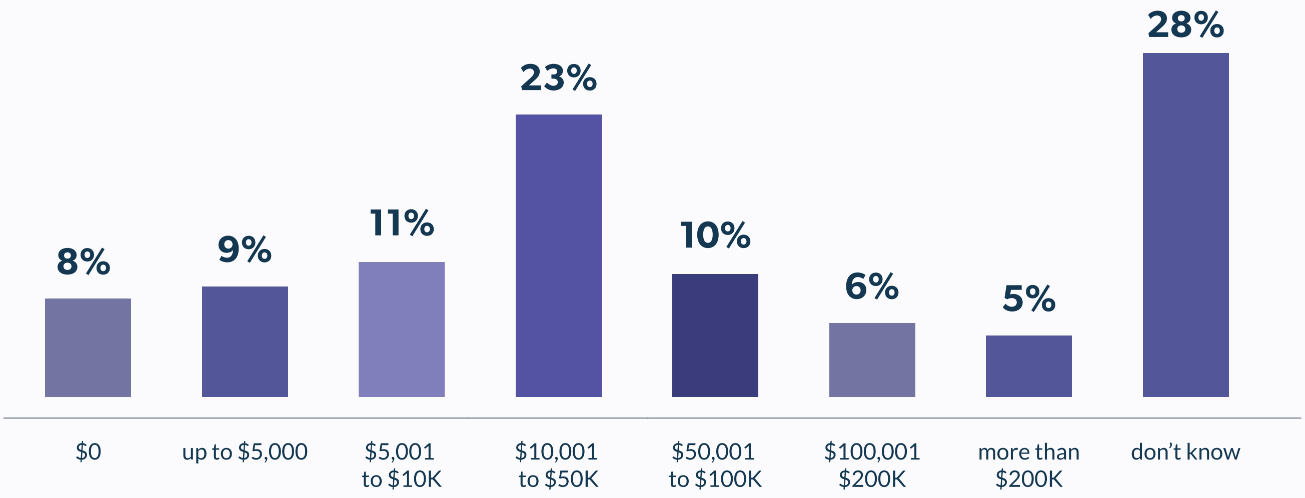
In this year's survey, a positive highlight was the shift in budget allocation to vendor management. In prior years, as many as 38% of organizations reported less than $10,000 in expenditure earmarked for vendor management… that's hardly enough to pay for an on-site visit, much less adequately invest in the robust practices required to do third-party risk management well.

> It's encouraging to see increased investments as now only 28% spend less than $10,000, with 44% of respondents now reported spending more than $10,000. That's a trend headed in the right direction.

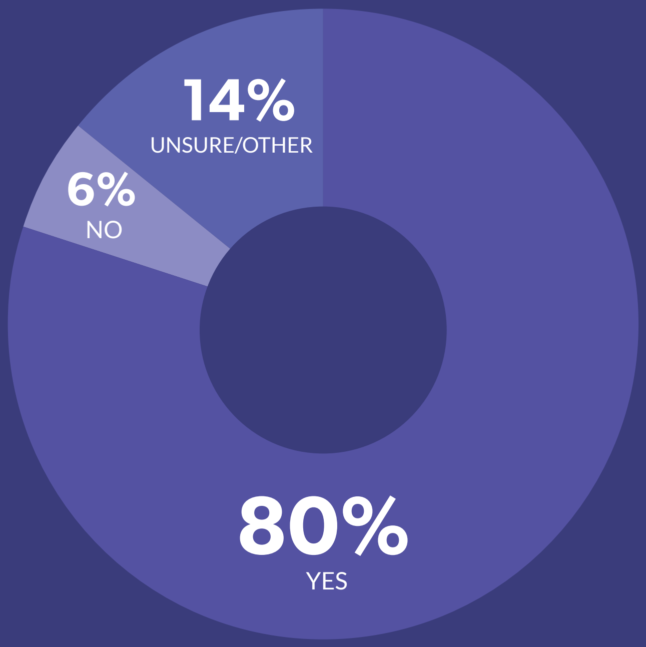
Aside from facilitating a well-functioning program, dedicating appropriate budget to vendor management shows regulators that you're committed to complying with regulations. They know, as do we, that complying with a third-party risk management policy with a consistent work product often requires investment. As noted in the prior result, this could be in the form of a full-time employee, budget for travel, documentation, outside expertise, legal opinions and even outsourcing portions of the vendor management process when needed.

In an era where both reputation risk and operational risk are so volatile, the investment of $50,000 or more seems warranted for most organizations, particularly those that can't afford a full-time employee to be handling the function in-house. The increased investment is one that we predict will continue in future years.

Besides full-time employees cost, how much budget has been dedicated to vendor management?



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



A common challenge for those in third-party risk has been proving to management the value behind investing time, dollars, employees and technology in vendor risk management. It's encouraging to see that in this survey, 80% of respondents believe that there is a positive return on investment. Equally important, the rate of those saying they do not see a positive influence has been cut in half since last year to only 6% of respondents.

Saving time and money is a more obvious benefit, but cost avoidance is another practical consideration – whether it's keeping an expensive contract from auto-renewing, or having real teeth in your service level agreements, there are many ways to reap real savings or avoid actual business disruptions through a well-managed program. We have included a large list later in this document of actual quotes from respondents on what their perspective is related to the benefits of vendor risk management.

Real Strategic Value

Tip: If you're struggling to get finance or senior management to realize the value, we recommend that you add up all the cost of your contracts with third parties and calculate 2.5% of that total cost. Take that number to management and explain that an average of 2.5% of vendor expenses is wasted a year on unintended auto-renewals.

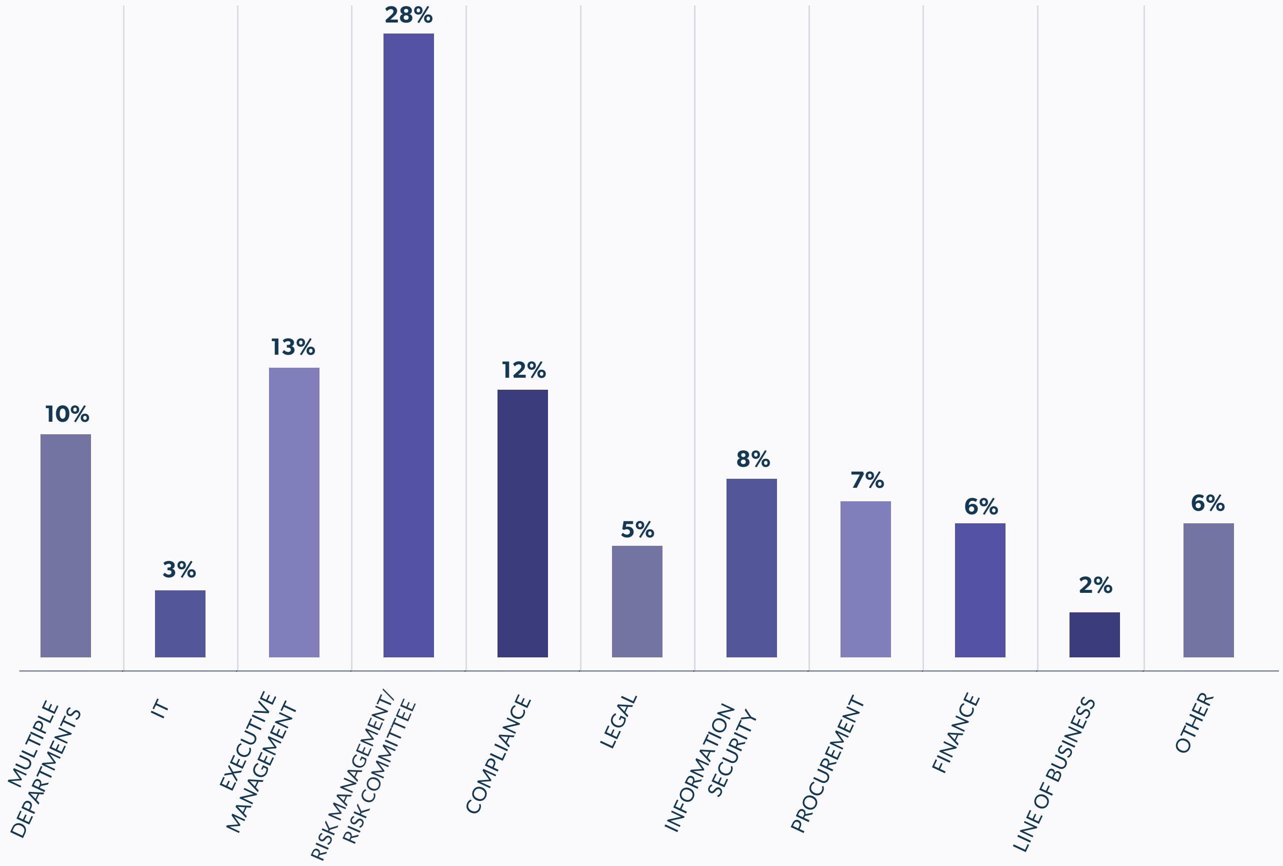
Organizational Structure

Independence from lines of business continues to improve and mature

Another step in the right direction this year is third-party risk management's increased independence from lines of business. Not only is it mandated in some industries, but it's also practical and incredibly important to the success of a healthy vendor management discipline.

Having an independent stance is important as third-party risk management should be risk-based and not totally beholden to business needs; and appropriate management requires an equal vote in all matters.

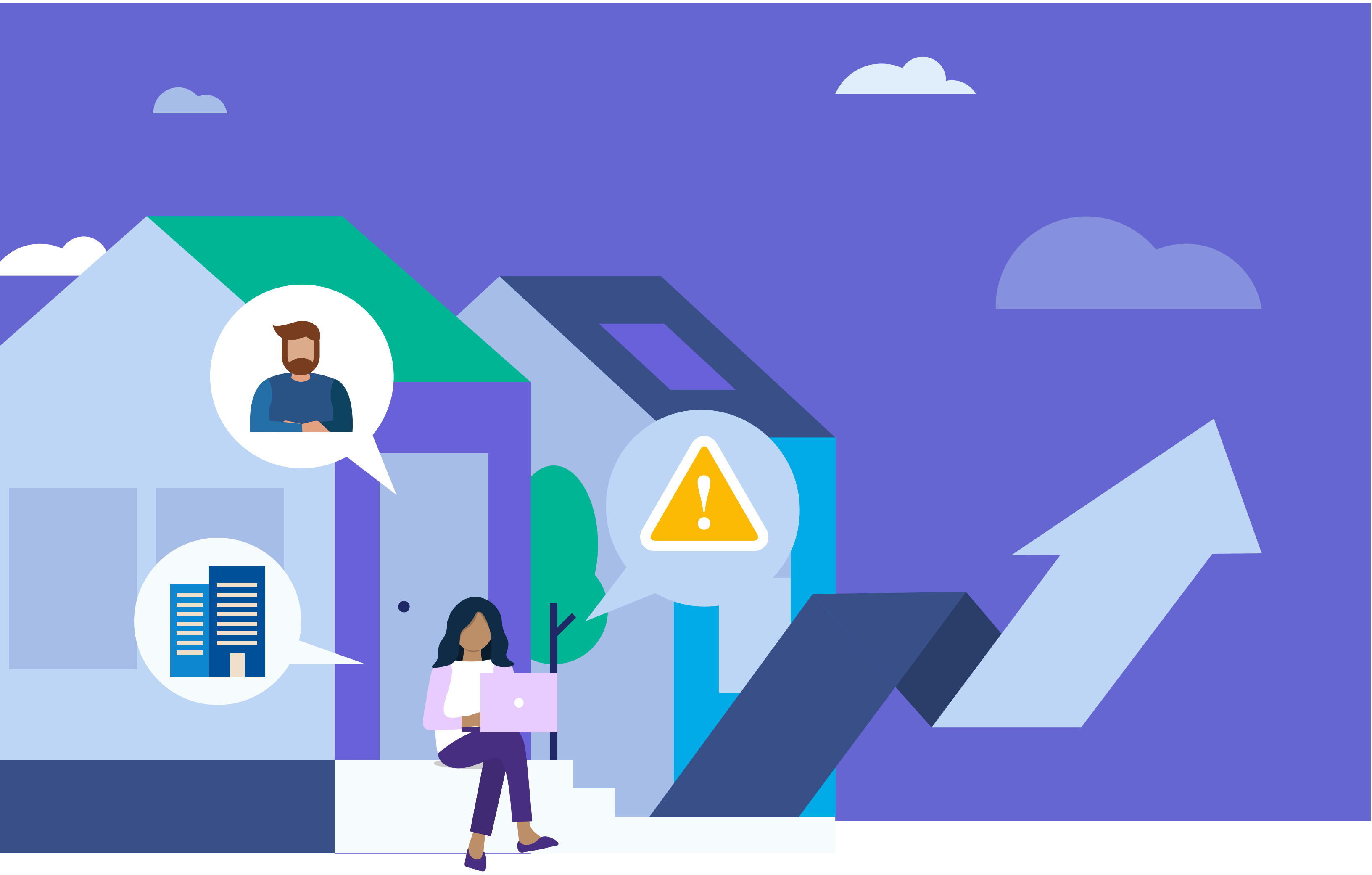
Where does vendor management report to?



As organizations mature, their delineation of risk and control functions from business unit functions has become equally clean.

Having the vendor management function independent helps further that cause, ensuring no one gets labeled as having “the fox guarding the henhouse” or yielding to a “favorite” vendor’s needs.

A few years ago, many organizations we surveyed had vendor management lumped in with Information Technology – in this year’s report, that’s down to only 8%. In terms of direct reporting to a line of business, that’s down to 2% – while we see the greatest representation, by far, at 28% reporting into the risk management function.



Sponsorship from the Top

Setting the tone from the top is important

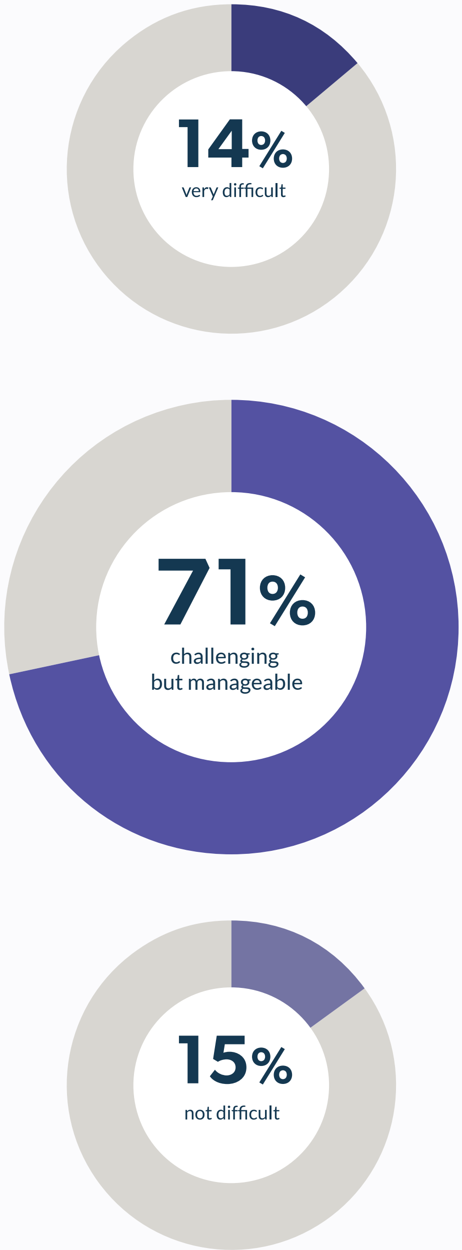
This result has not changed much over prior years – with 71% (slightly more than previous years) finding it challenging to secure business unit support for third-party risk management but manageable. Fourteen percent (14%) find it very difficult and 15% said it's not difficult at all.

We believe that in 2021, securing business unit support will continue to increase as employee awareness grows and the importance of an adequate program becomes more mainstream and discussed.

> The pandemic has been a time where all employees became much more conscious of how business works remotely and aware in the increased reliance (and trust) each organization has on third parties.

Of course, this comes with a need to communicate practically with leaders and decision makers in your organization. In this time of heightened awareness, it may be the right time to do a bit of lobbying on behalf of vendor management and examine what has been going well during the pandemic and what challenges remain that you could use additional support.

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



Size and Makeup of Vendor Landscape

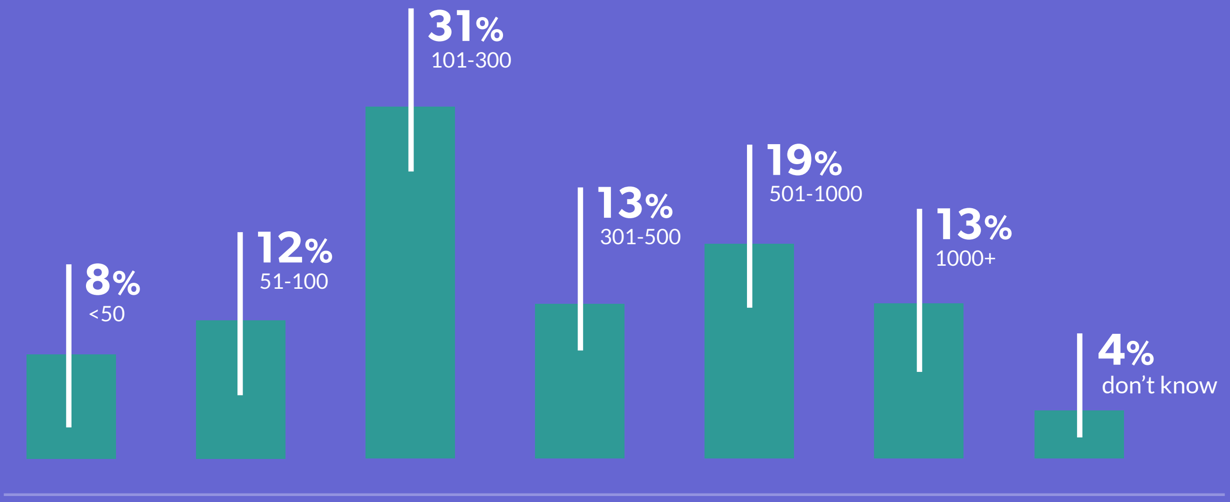
At most companies, vendor management is complex

This response isn't necessarily indicative of the size of the organization responding, because there are also varying degrees in which the organization outsources functions. Does the organization embrace outsourcing everything or just certain functions they may not be able to adequately staff in-house? Often, some of the larger organizations outsource to less companies than you'd expect as many tend to have the resources to throw an army of people at projects to build their own infraustructure.

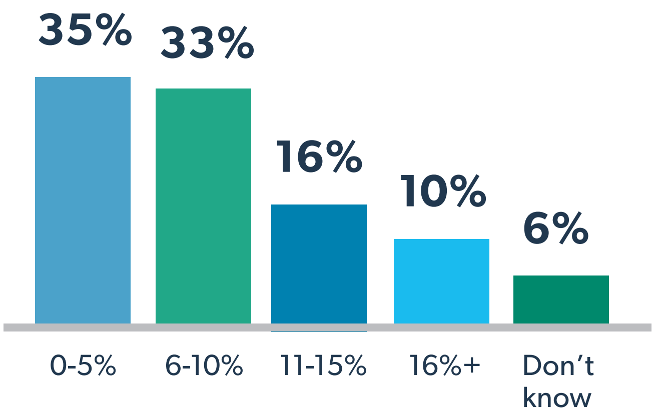
Remember, as you outsource and continue to improve your vendor management functions, be sure that your list of vendors is comprehensive and reasonable. While larger organizations may have the ability to keep more functions in-house, they're also more prone to duplicate services and suppliers across different verticles. This can often lead to excess spending due to haphazard vendor management.

The vast majority of respondents – nearly two-thirds – report that they have between 100 and 1,000 third-party providers. We also know that of these organizations, two-thirds had two or less employees to handle the tasks. This tells us that there's a good chance that third-party risk management continues to be fairly under-staffed.

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



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



In this year's survey, more than half of respondents say their critical vendors make up 10% or less of their vendor population. This is in line with expectations and best practices. Those who report that more than 15% of their vendors are critical and 6% who aren't sure, we suggest revisiting how many core services are outsourced and how aggressively they need to be managed.

In 2020, many third-party risk professionals likely gained a much better perspective and appreciation for which third parties are critical as you had to rely on them remotely. Determining vendor criticality is incredibly important as it drives deeper due diligence, more informed contracts and requires consideration on how to "stand in" to minimize disruption to your business and your customers.

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 there be a negative impact to your organization?*

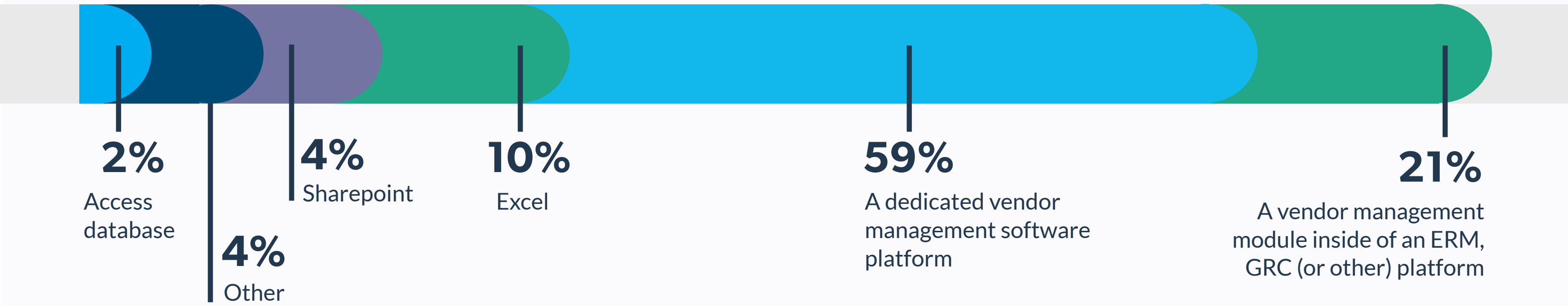
If any of these are "yes", that should be considered a critical vendor.

Technology Tools Used

High number using dedicated platforms

Almost 60% of respondents said they now use a dedicated vendor management software platform. Reviewing hundreds of data points for hundreds of vendors in order to calculate an inherent and residual risk is no small task for a normal human brain. We're also required to track the process of hundreds of risk assessments with input from various internal and external parties. It's no wonder more and more organizations are opting to get some support from software.

What is your primary tool for managing your vendors?



It's important to consider using tools built to do vendor management specifically, and one that is able to accommodate the complexities of your organization. For those using enterprise risk management (ERM) or governance, risk management and compliance (GRC) applications, those solutions are often built to manage the overall risk of the organization and are not always equipped to manage the complex and often specialized assessment requirements associated with outsourcing.

Oftentimes, they require large investment of resources for customization, meaning money, time, talent, which all adds up. Dedicated platforms designed for vendor management allow the ability to leverage best practices across the industry and provide a more accurate and timely assessment process.

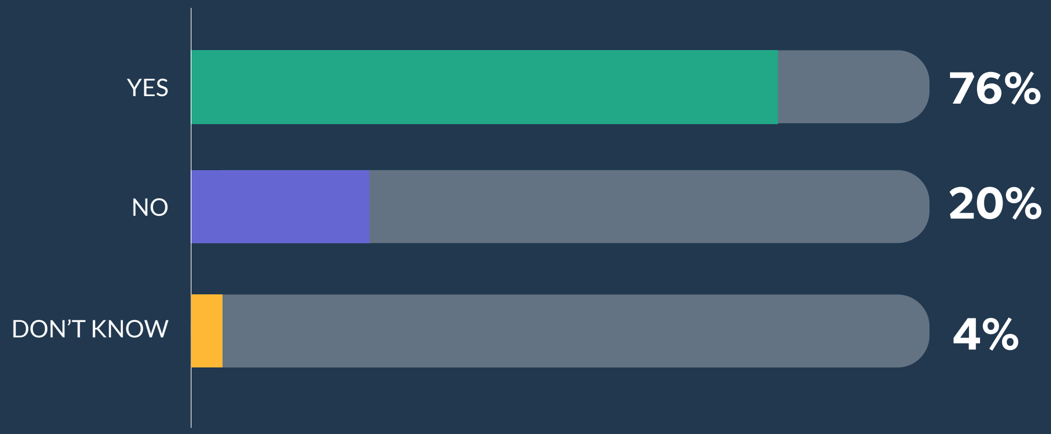
Best Practices in Vendor Management

A story in continued improvement

It’s good to see that 76% of respondents have a formal process for determining inherent and residual risk. This means that we’re trending in the right direction and are not only making assessments on vendors prior to signing an agreement, but that there are systematic practices in place to do so.

This aligns with overall best practices and most regulatory requirements on the matter.

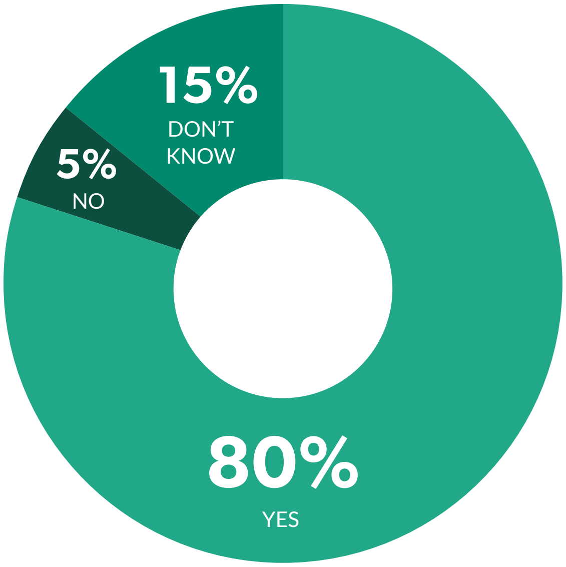
Do you have formal risk assessment processes in place to determine inherent risk and residual risk for all new vendors pre-contract?



Eighty percent (80%) 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. What's interesting is that this number is slightly higher than those who conduct a risk assessment. What this tells us is that there is a larger emphasis on determining criticality than there currently is on conducting a full risk assessment, which is understandable. We all have to start somewhere, and starting with knowing who your show-stoppers are is definitely the way to go.

As a reminder, criticality and risk are NOT synonymous. A vendor who is high risk isn't necessarily critical, and a critical vendor could be low risk.

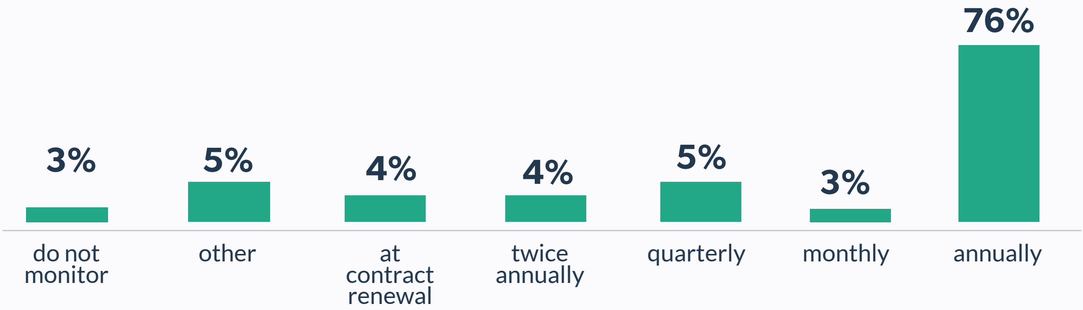
Do you have a formal process in place to determine criticality for all new vendors pre-contract?



Eighty-eight percent (88%) of respondents said they're reviewing their high-risk or critical vendors at least annually, which is great. For those waiting for a contract renewal with a critical or high-risk third party, or not updating the records at all, it's important to be aware that you're in danger of missing something that could drastically impact your organization, or worse, your customers.

Periodic assessments of your vendor's control environment is an integral part of the third-party risk management process, especially for critical or inherently high-risk vendors. Furthermore, if a vendor's control environment changes dramatically, you catch wind of something amiss or if the role they're playing with your organization changes, it's time to re-assess the risk and business impact they pose to your organization. Remember, risk isn't tied to a calendar, so as issues emerge, address them in a timely manner rather than waiting for an arbitrary scheduled review date.

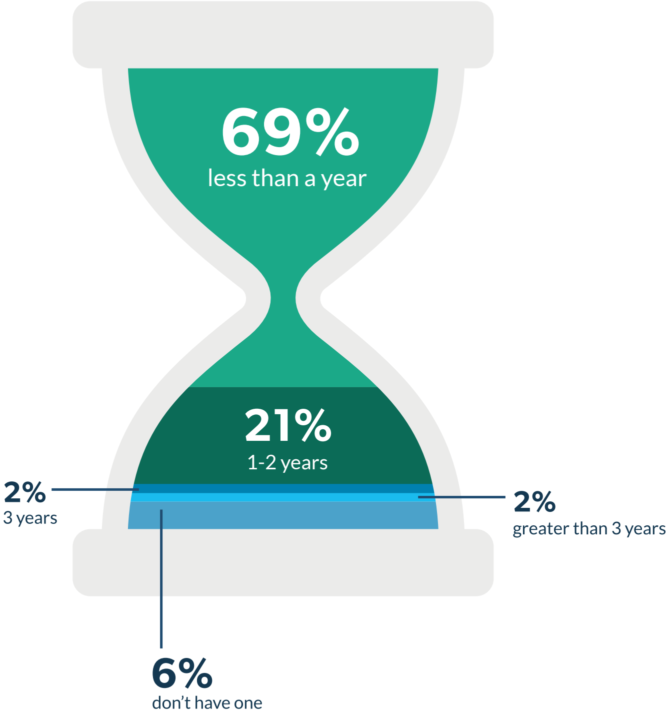
How often are you reviewing/analyzing your high-risk or critical vendor documentation?



Keeping your vendor management policy documents up to date and consistent with regulatory guidance and best practices is incredibly vital to having a successful program. It's encouraging to see almost 70% are updating their vendor management policy annually.

The vendor management policy, like any other policy, should be updated regularly, particularly as new guidance comes out or something significant changes in a business structure or processes. Did you know that referencing outdated guidance is often an audit finding? Updating policies at least annually isn't only a best practice, but it's also a baseline expectation. Incorporate any relevant changes, present it to the proper authority for reapproval and recirculate in your system of record.

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



Operating Models

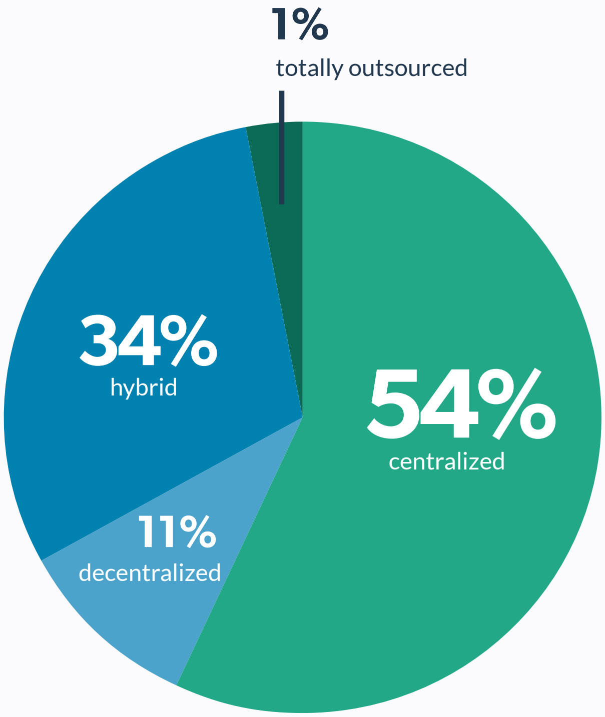
More than half of respondents have a centralized model again in this year's survey

The exact parameters of what vendor management models entail can certainly vary, but let's assume that we're referring to all third-party risk management functions conducted by the same dedicated team (centralized), shared functions between a dedicated team and other departments (hybrid) or third-party risk management functions managed throughout different areas without a dedicated team (decentralized).

This year, over 50% of the respondents indicate that they're using a centralized model and 34% are hybrid. This is good, considering these are the two models we've found seem to have the most efficient, practical and compliant programs. In a decentralized model, which comprised 11% of our sample base, there's often much inconsistency fulfilling third-party risk requirements, many loose ends and trouble getting holistic reporting to decision makers. Furthermore, those charged with third-party risk management often feel the wear and tear of task saturation, as they have additional priorities beyond vendor risk management.

Finally, one percent stated that they're totally outsourcing vendor risk management. Unfortunately, this approach isn't practical and almost impossible to achieve compliance. Outsourced services and functions are veins tightly woven throughout all areas of an organization. There is so much communication and information sharing needed to get the job done right, its impossible to rely completely on an outside vendor to do it for you.

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



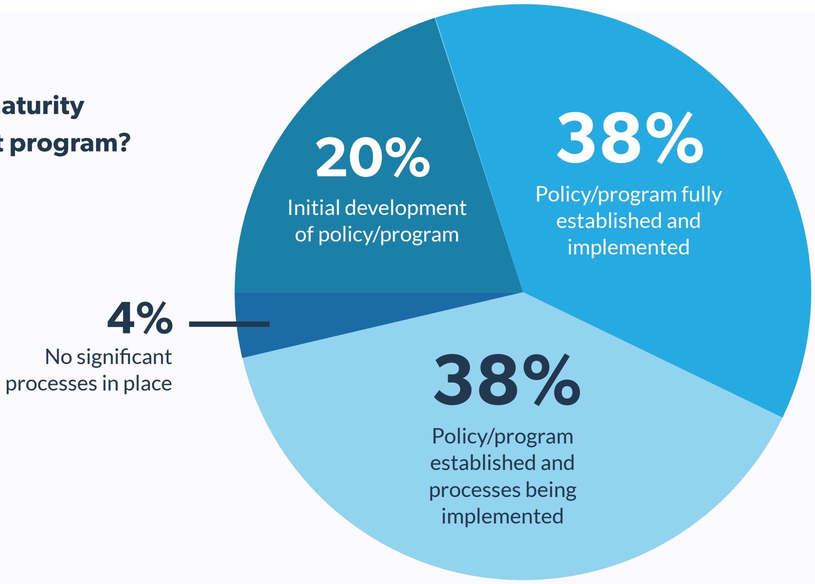
Maturity of Vendor Management Programs

The trend towards program maturity continues with very impressive progress

To determine an overall trend of maturity, we asked respondents to estimate the maturity level of their vendor management program. Over three quarters – 76% – report significant progress or having reached the desired state which is terrific and represents achievement, control and the opportunity to be reflective and look for ways to continue to model best practices. Broadly speaking, there really hasn't been substantive changes to regulations pertaining specifically to third-party risk management practices. This could be why some organizations have had the opportunity to make progress in their overall maturity.

For those still working their way to their desired state, there are many resources available to assist and to continue to mature your program. Webinars, whitepapers/eBooks and online communities are great places to learn the best practices from peers and to incorporate them into your program. Equally important, documenting out a project plan and measuring progress against those tasks will provide real evidence in an examination that you're taking a proactive approach to addressing deficiencies and creating a pathway for a fully mature program.

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



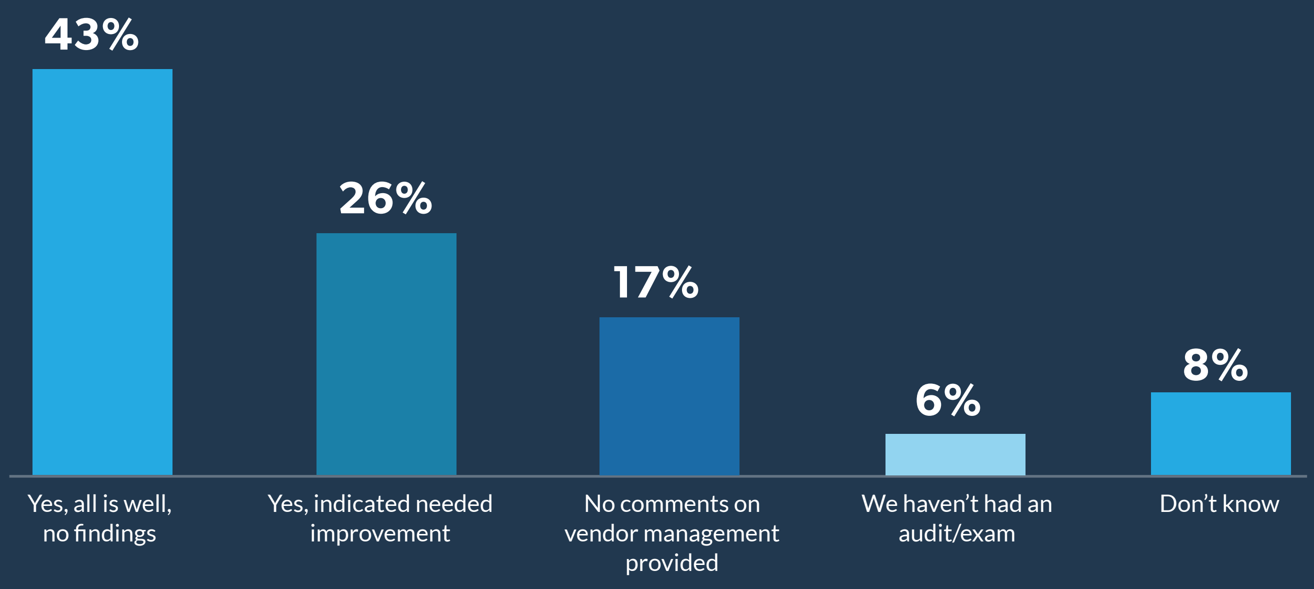
Regulatory Focus and Exams/Audit Results

Evidence of continued regulatory focus on vendor management

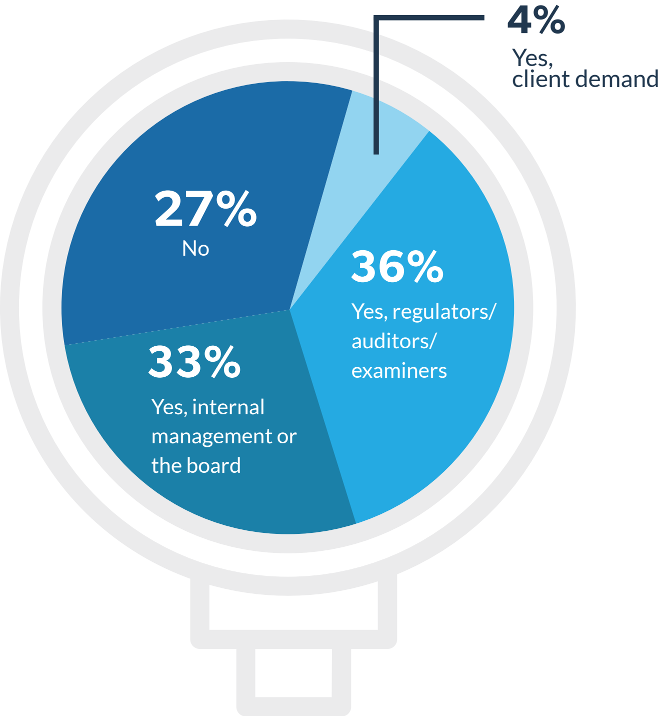
It's good to see that almost half of our sample base has a program in place which satisfies audit requirements, and perhaps 17% more, assuming "no comment" means everything is okay (and in audits, that is often the case). This also shows that one-third has some room for improvement, most of which was confirmed by audit feedback.

A third-party risk management program doesn't just answer to an exam or audit cycle, as that's often a surface-level annual "health check". The real measure should be the day-to-day ability to prevent third-party risk from creating dangers to the business. Use any opportunity presented to conduct your own health check. You may not be able to solve every problem, but you can recognize them, analyze the situations, determine plans and demonstrate progress. The best time for a check-up is when things are going well, not when things are obviously falling apart.

During your last exam/audit, did your regulator/auditors provide feedback on your current vendor management program?



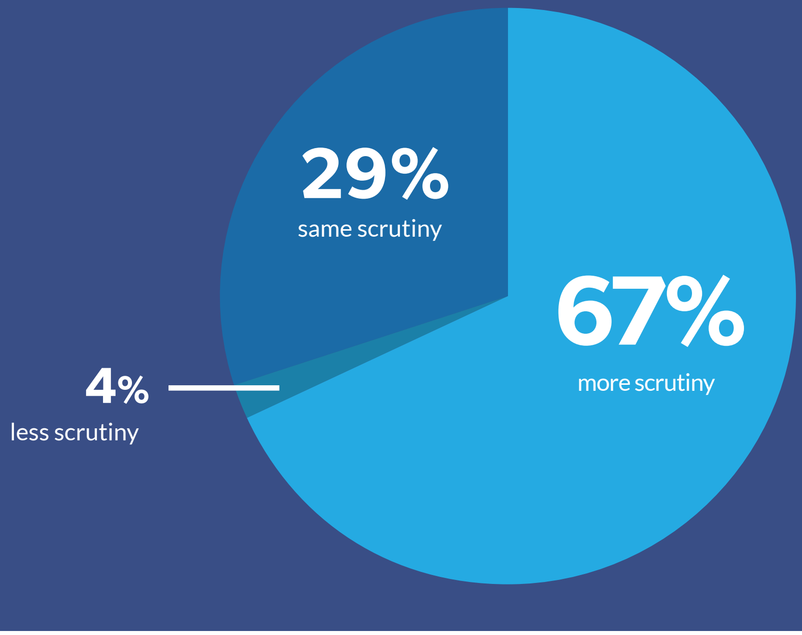
Are you feeling pressure to improve your vendor management program? If yes, what is the source?



Not surprisingly, over three quarters of our sample base told us that they ARE feeling pressure to improve their program, partially because of regulatory/audit scrutiny, and slightly less because of internal management/board feedback. While we don't actually know whether the 27% not feeling pressure are smooth sailing because their practice is sound, or because no one is paying attention, it's safe to say that there is increasing pressure, overall, on third-party risk management.

In an era of data breaches and so many smaller service providers struggling in the current pandemic world, it's natural that both internal and external forces will want to see what organizations are doing to manage their third parties effectively and ensure their reputation and data are safe.

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



Sixty-seven percent (67%) of the respondent organizations feel that there is more scrutiny on third-party risk management over the last year. Let's consider that the previous year, 71% said the same thing. This tells us two things:

1. **Scrutiny on third-party risk management is generally not going anywhere and continues to be on the rise. We in vendor management know this. We know that this is a best practice for a reason. All the regulatory updates we see seem to only add more accountability rather than change the way we know we should go about this.**

2. **While it's evident that scrutiny is overall on the rise, there may have been some things in the last year which have caused more people to feel pressure in other areas as well.**

Bad things happen, and we're never totally free of risk. However, there are very real negative consequences if an organization's third party is breached, and they're found to have not done their due diligence in accordance with regulatory guidance — from enforcement actions to fines, and of course reputational damage. It's important to be aware that third-party risk is not defined by a headline event or a cybersecurity incident, but it's absolutely informed by both — by that standard, staying abreast of industry developments and regulatory expectations should be duly considered when setting the bar for your own program.

Vendor Management Challenges

Internal resources are being stretched thin

Having enough internal resources	**40%**
Getting the right documents from vendors	**39%**
Time management	**32%**
Automating the process	**26%**
Tailoring our due diligence requests to be appropriate for each vendor	**25%**
Completing risk assessments	**23%**
Keeping track of all the documents and data	**17%**
Managing contracts and negotiations	**13%**
Knowing who our vendors are	**11%**
Garnering senior management support	**10%**

Analyzing SOC reports	**8%**
Determining which vendors are critical to our organization	**8%**
Preparing for exams/audits	**8%**
Obtaining adequate budget	**7%**
Awareness of our vendor's cybersecurity	**7%**
Keeping up with the regulations	**6%**
Other	**6%**
Completing a financial analysis	**5%**
Reporting	**5%**
Keeping senior management informed	**4%**

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

Now here we continue to see the most significant trend and point of note in our State of Third-Party Risk Management 2021: **the number 1 challenge for vendor risk management is having enough internal resources to support the program.**

Organizations are lacking on dedicated full-time employees and funding for vendor management. This, in combination with increased pressure, shows us that something has got to give. There may also be a significant lack in credentialed and experienced expertise to get the job done well. Not surprisingly, following closely behind are the resulting issues of struggling to collect documents and conduct risk assessments, adequately managing time, finding the right ways to automate the process and tailor due diligence in a way that leverages avalable resources and adds significant value.

Addressing these challenges requires creativity – either investing more in internal resources, outsourcing more control functions, hiring the right experts, finding different ways to gather documents, outsourcing assessments to subject matter experts either internally or externally can all go a long ways toward alleviating these pain points.

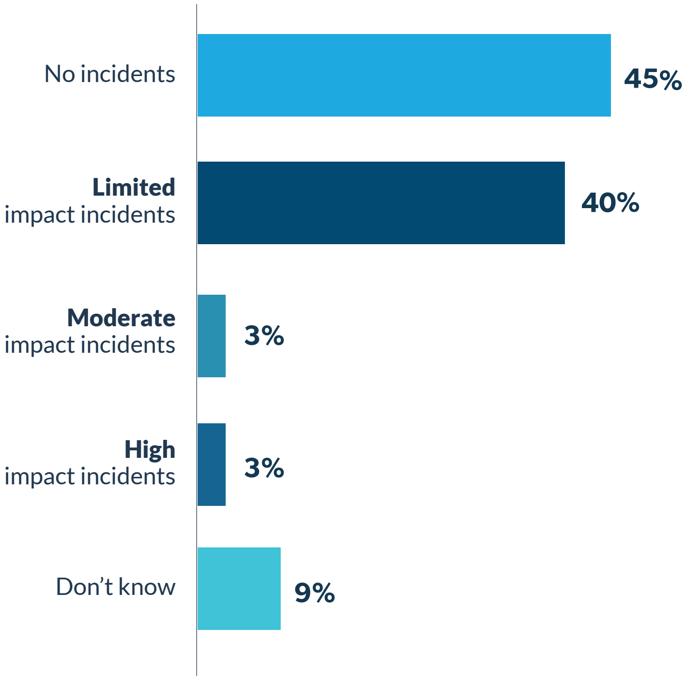
Pandemic Impact on Third-Party Risk Management

A mixed bag of results

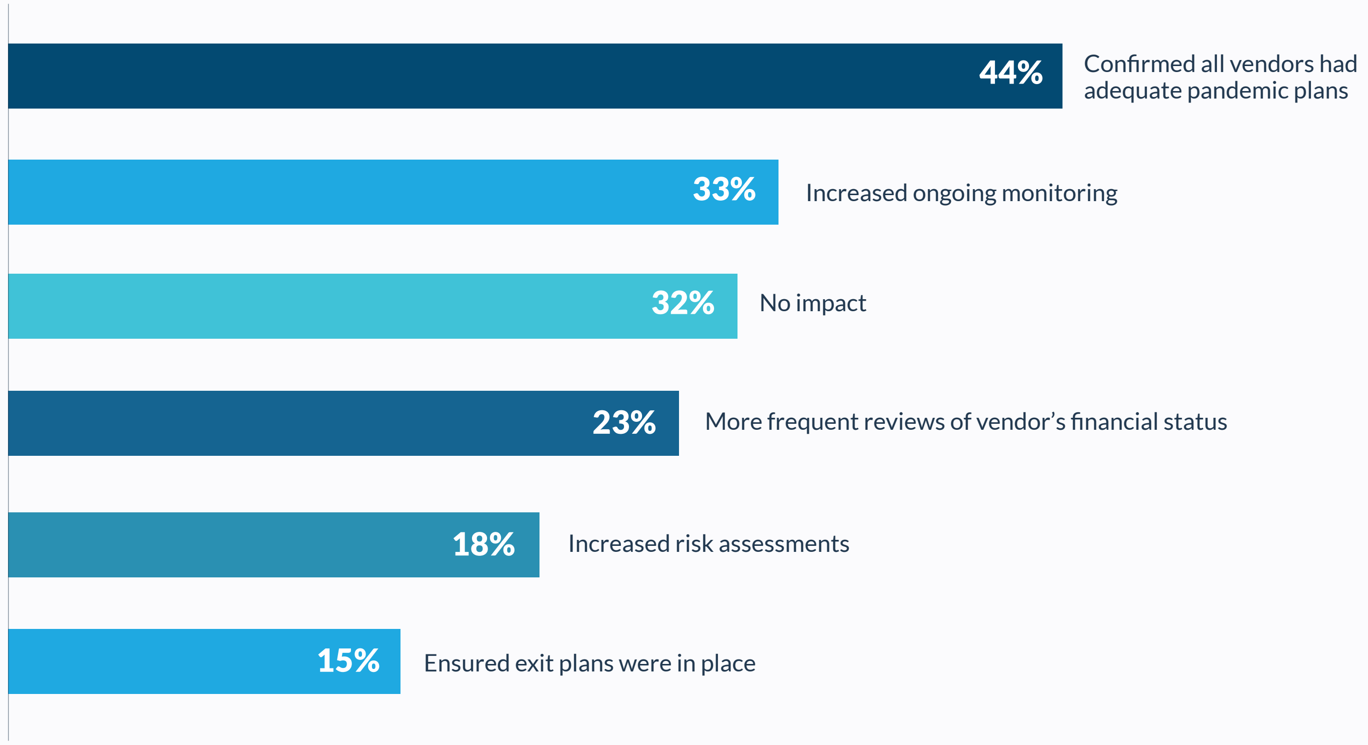
The rippling, negative affects of the 2020 COVID-19 shutdown came on fast and are still being felt. Business was running as usual one day, and perhaps a week later, everyone was working remotely, if they were lucky enough to be working at all. As with any unpredictable and rapidly executed response plan, the path was laid out for mishaps, breaches and malicious cyber activity.

Nearly half of respondents experienced a cybersecurity incident of some kind in 2020. Luckily, most of those were low impact. We should all keep in mind the importance of documenting not only your path to recovery, but also taking time to evaluate and learn from lessons learned.

Did you experience third-party cyber incidents during 2020?



How has the COVID-19 pandemic impacted your vendor management processes?



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

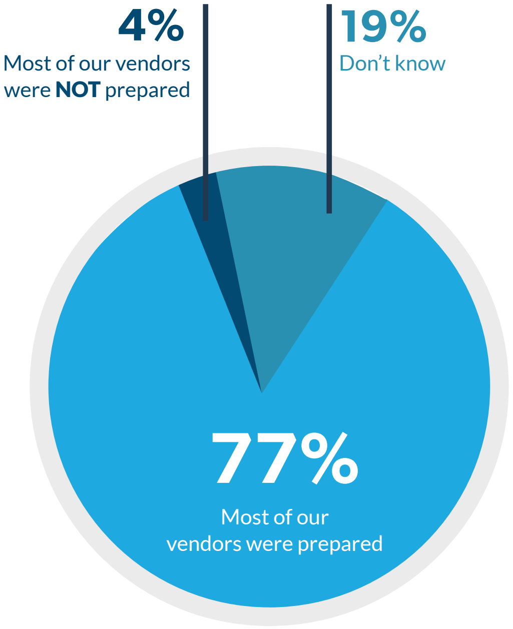
Incidents aside, how have the events of the last year impacted programs themselves? Two thirds of our sample took measures to be sure their organization was protected. Fourty-four percent (44%) ensured their vendors had adequate pandemic plans in place, 33% increased their ongoing monitoring, 23% decided to increase the frequency of their reviews of financial status, 18% increased risk assessments and 15% ensured exit strategies were in place.

> These are all good measures to take, and the additional attention will only prove beneficial on our road to recovery.

It's important to remember that not all of the shutdown fall-out is felt instantaneously. There may be organizations holding on now, but sustainability is uncertain.

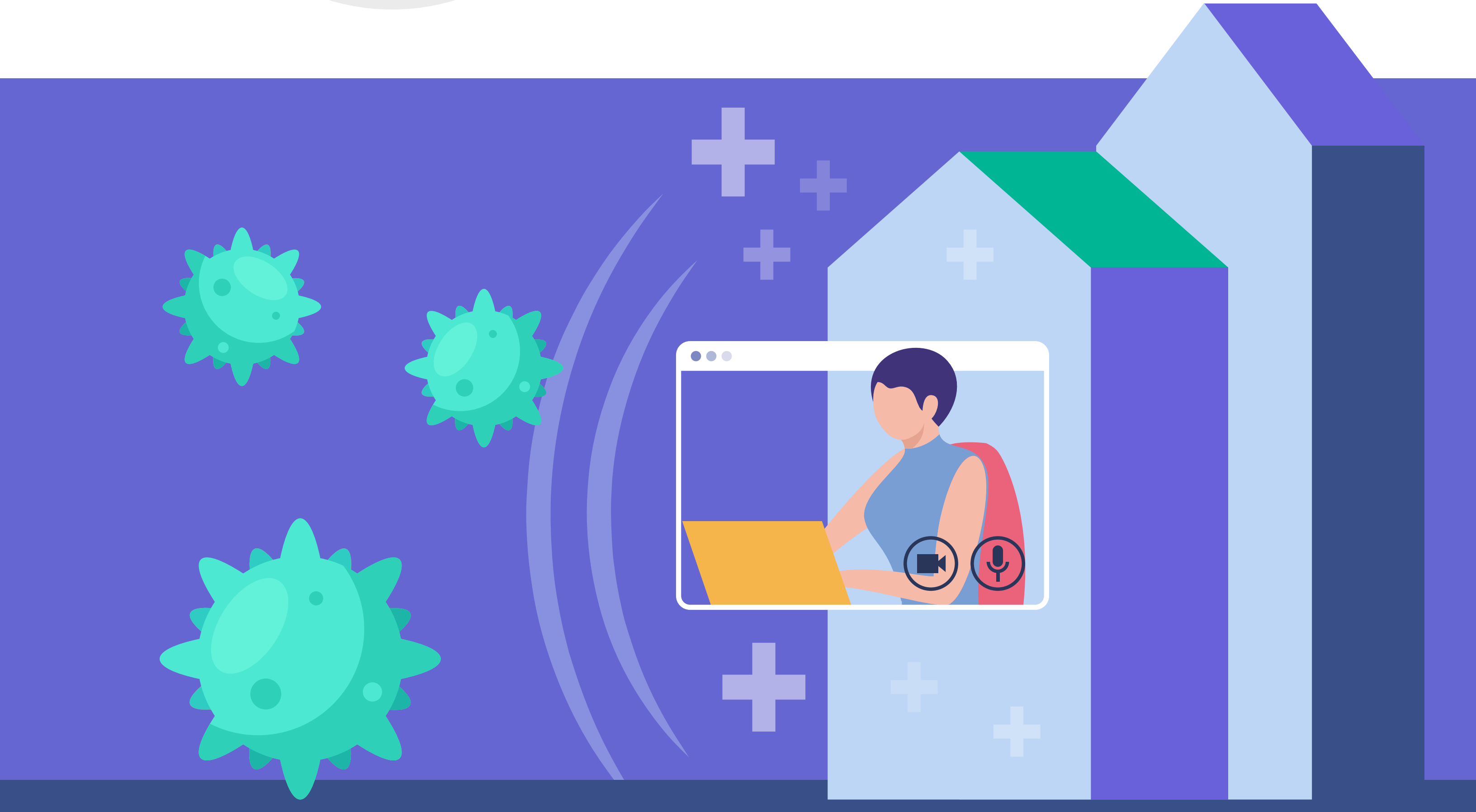
Even when operations begin to go back to normal, the residual impacts to organizations large and small will continue to play out over the coming months and years.

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?



It's comforting to know, though, that 77% of respondents saying that the majority of their vendors were prepared and implemented their pandemic plans without issues. Only 4% felt their vendors were not prepared or had no pandemic plan in place, and they were negatively impacted.

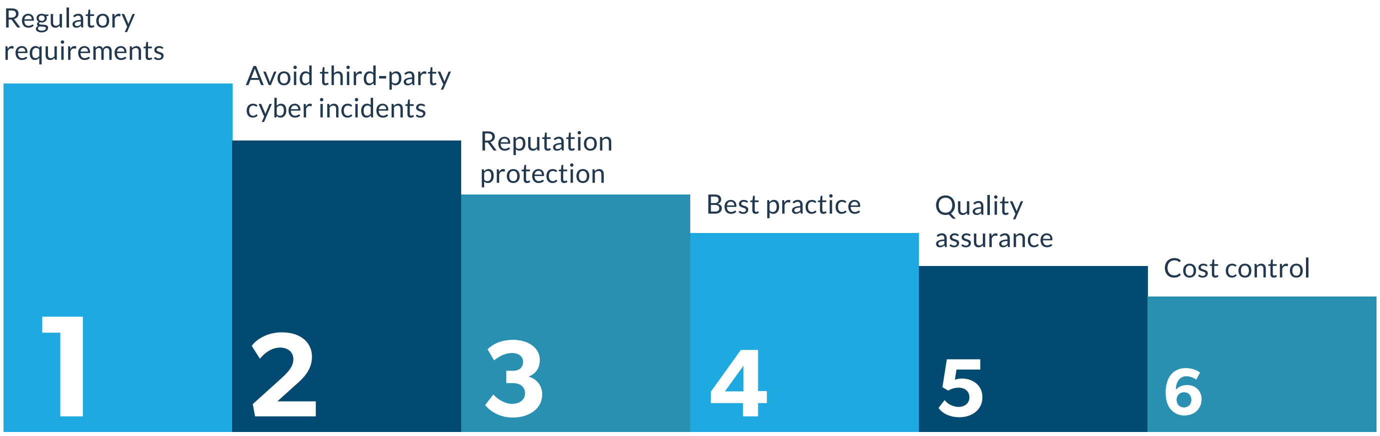
As we said before, there are some things that even the best thoughtout plans aren't prepared for. It's important to look into these matters and determine the root cause and if circumstances could have been avoidable. Of course, this is after dealing with the immediate impacts. Perhaps the vendor is no longer able to provide services and a contingency plan of your own is necessary. Perhaps the matter was recovered but there are systemic issues which show further action should be taken to remediate, or perhaps transition to a new vendor. Either way, keep a close eye, increase ongoing monitoring and incorporate lessons learned.



Primary Benefits

Why we do what we do

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



Not surprisingly, the primary reasons organizations are conducting vendor risk management is to meet regulatory requirements and protect their organization. This falls in line with the other results of our survey.

We all know that this is a best practice that ultimately protects from incidents, reputation damage and excess spending… but it often takes that big brother to hold us to the fire before resources are dedicated to a non-revenue generating function.

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.

Risk reduction at initial vendor selection. Risk reduction through monitoring and renegotiating or terminating vendor relationships.
Getting ahead of issues through monitoring.
Government, 5001+ employees

Cost effectiveness.
Bank, $1B to $10B

An **important component** of our overall IT security framework.
Education, 5001+ employees

Gives our business stakeholders **more information about their vendors** and knowledge to make better business decisions when engaging with vendors.
Healthcare, 5001+ employees

Understanding our risk of outsourcing.
Bank, $10B+

Identifying and excluding those companies whose practices **put us at risk of penalty or loss**.
Lender, 1001-5000 employees

Security, **peace of mind**.
Bank, Less than $1B

Responsible growth and regulatory/legal compliance.
Bank, $10B+

The ability to identify Business Continuity risks, Information Security risks and Data Privacy risks amongst our vendors.
Wealth/Asset Management, 251-500 employees

Insight information about vendors to **help my organization make an informed decision** to partner with specific vendors.
Retail, 5001+ employees

Understanding about what type of risk is caused by vendors, better discipline over vendor performance and tighter adherence to complimentary controls required by key vendors.
Bank, $1B to $10B

Organization of files, due diligence and decreased risk.
Insurance, 1-100 employees

Cost efficiency and risk management.
Fintech, 501-1000 employees

Understanding vendor risk as it impacts our business functions.
Lender, 5001+ employees

Opportunity to **evaluate the performance** of each vendor.
Credit Union, Less than $1B

Transparency and accountability.
Bank, $1B to $10B

The ability to apply **adequate protections to our data** as/when we share our data with third parties.
Telecommunications, 5001+ employees

Stronger risk management.
Healthcare, 5001+ employees

Secure company from external threats. Maintaining company reputation and customer trust.
Insurance, 5001+ employees

Full lifecycle of vendor management and audit trail.
Manufacturing, 5001+ employees

Visibility into risks that our vendors pose to our company, and once our program matures, understanding of supply chain gaps.
Human Capital Management, 1001-5000 employees

Financial benefit, regulatory compliance as well as time savings in the form of avoiding litigation, saving wasted employee time dealing with vendor risk issues, etc.
Mortgage, 251-500 employees

Mitigating risk exposure from external sources.
Healthcare, 5001+ employees

Regulatory compliance and vendor knowledge to assist in decision making.
Bank, $1B to $10B

Provides due diligence and assessment information to the business to assess risk prior to engaging the relationship, contract management to ensure company and customer protections are in place and ongoing oversight of high-risk relationships to ensure they're meeting company expectations.
Lender, 5001+ employees

This is a regulatory requirement and third-party vendors **do carry risk that should be mitigated**.
Insurance, 501-1000 employees

Reducing risk, primarily compliance and reputation, and cost savings because of proper contract management.
Credit Union, Less than $1B

Ensuring that third parties have **sound controls to mitigate risk** helps create a safe institution.
Bank, $10B+

Main concern is invoice/ contract management — cost benefit for managing canceling contracts properly.
Fintech, 1-100 employees

Tracking contract dates. Inventory of contracts and vendors. Help focus on higher risk vendors.
Credit Union, Less than $1B

Ability to assess and manage risk associated with **utilizing outside vendors.**
Insurance, 101-250 employees

Protect us from vendor risk and errors in managing vendor relationship.
Lender, 1001-5000 employees

Ability to **manage risk.**
Bank, $1B to $10B

Safety and soundness for member data shared with vendors and SOC analysis.
Credit Union, Less than $1B

NPI security and **mitigated risk.**
Bank, Less than $1B

Creditable support to NCUA examiners of Vendor Management Review.
Credit Union, Less than $1B

Mitigation of operational interruption risk and **better control of procurement** and third-party contracting.
Bank, $1B to $10B

Visibility.
Brokerage, 5001+ employees

Maintain compliance, reduces risk, **reduces cost.**
Bank, $1B to $10B

Vendor Risk Management is **extremely vital because vendors are a key part** of our organization.
Bank, $10B+

Business — How we select, what we expect and what we track matters.
Regulatory — Regulators require a management plan and adherence to the plan; **exams review our performance.**
Bank, $1B to $10B

Opportunity to reduce risk to the bank.
Bank, $1B to $10B

Overall **protection of the company** itself.
Mortgage Lender, 501-1000 employees

Organization, control and risk management.
Mortgage Company, 101-250 employees

Security and **centralized information** to make decisions.
Insurance, 101-250 employees

Insight to our risk levels, **storage of contract, terms and reporting.**
Bank, $10B+

Organization, reporting for vendors — one central location for documentation — peace of mind.
Fintech, 501-1000 employees

Satisfying the regulators.
Bank, $1B to $10B

Consistent due diligence and assessments.
Bank, $10B+

Proper contract management and **proper vendor due diligence.**
Credit Union, Less than $1B

Satisfies regulators.
Mortgage Lender, 501-1000 employees .

Protection from risk.
Bank, Less than $1B

Reduced risk from a performance/SLA perspective, data sharing, data management and vendor relationship management and continuity.
Healthcare, 101-250 employees

Reduce third-party risks.
Bank, $10B+

Accurate representation of who we work with, what information we share, whether a vendor is performing as expected, etc.
Credit Union, $1B to $10B

Security and reliability of third-party relationships.
Bank, $1B to $10B

Adequately capture risk and mitigate risk accordingly; **keeping track of SLAs.**
Bank, $1B to $10B

Reduction of third-party risk exposure.
Retail, 5001+ employees

Regulatory compliance and **mitigated risk.**
Bank, $1B to $10B

Risk identification.
Healthcare, 1001-5000 employees

Risk mitigation/**regulatory responsibility.**
Fintech, 1001-5000 employees

Awareness of risk when making decisions.
Mortgage Company, 1001-5000 employees

View into risks.
Insurance, 5001+ employees

It **protects the organization** from engaging vendors without appropriate controls.
Bank, Less than $1B

Knowledge of the risks associated with each of the vendors we work with. **Tools and procedures to ensure ongoing oversight and monitoring** of the relationships.
Insurance, 501-1000 employees

Risk management gives our organization the confidence that **our documents are secure.**
Credit Union, $10B+

Better pricing / reduced risk.
Mortgage, 1001-5000 employees

Assists in preventing company from doing business with bad companies and ensures vendors are performing to their expectations.
Insurance, 1001-5000 employees

Helps surface potential vendor issues before they become critical; helps provide more information when we are conducting searches for new vendors.
Wealth/Asset Management, 1-100 employees

Reduced data breach and ISO27001 accreditation.
Telecommunications, 5001+ employees

Reduced risk.
Government, 5001+ employees

Reduces InfoSec **exposure.**
Retail, 1001-5000 employees

Monitor critical and high-risk vendors effectively. **Ensure at least minimal due diligence.** Advise and support departments in vendor management.
Bank, $10B+

It safeguards our brand/ reputation, customers and annual overhead.
Bank, $1B to $10B

Mitigation of risk and increased insight.
Education, 5001+ employees

Protects the organization.
Lender, 501-1000 employees

Centralized contract/vendor information; **knowledge of vendor reliability.**
Bank, Less than $1B

Control over risk. The benefit of evaluating vendors and their performance which gives us the tools to cut ties before renewing bad contracts and the possibility of combining services to existing vendors to save money.
Credit Union, $1B to $10B

Visibility into the tools being used across the business to **better understand the presented risk from a legal, security and privacy standpoint.** This also allows to help ensure we are in compliance with any applicable regulations.
Fintech, 1001-5000 employees

Confidence in our critical and non-critical vendors.
Credit Union, $1B to $10B

Meeting regulatory and client expectations for **robust onboarding and oversight** to mitigate risk.
Mortgage, 1001-5000 employees

Gives the bank an idea of where the risk lies.
Bank, $1B to $10B.

Many areas and can't live without: **All kinds of due diligence is needed.**
Bank, $10B+

Understanding our risks with each vendor and negotiating better contracts based on the due diligence results.
Credit Union, $1B to $10B

Compliance.
Fintech, 1-100 employees

Avoiding financial loss, project delays and reputation damage.
Healthcare, 501-1000 employees

Control over risk. The benefit of evaluating vendors and their performance which **gives us the tools to cut ties before renewing bad contracts** and the possibility of combining services to existing vendors to save money.
Credit Union, $1B to $10B

Minimizes risk and satisfies the regulatory requirements.
Credit Union, $1B to $10B

You cannot manage what you can't organize and quantify.
Lender, 101-250 employees

Compliance and security. (And, **we could not complete our SOC reports without it!**)
Fintech, 251-500 employees

Risk management.
Bank, Less than $1B

Minimize the risk (financial, reputational and legal) to the organization by **ensuring each third party that we are conducting business with are reviewed for potential loss.**
Bank, $1B to $10B

Visibility into risks.
Automotive, 1001-5000 employees

It helps centralize the information into one area for consistency and allows us to remain in compliance with all of the regulating authorities.
Insurance, 251-500 employees

Ensuring all potential risks are mitigated while **protecting the organization from unnecessary exposure to reputation damage,** security break and regulatory fines and penalties.
Bank, $10B+

Assessing and managing the potential risks from vendors.
Credit Union, $10B+

Vetting vendors and enhancing security.
Bank, Less than $1B

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

Vendor risk management is an intangible asset. **Helps to detect and prevent unknown risks**, avoid nasty surprises and protect the institution's reputation.
Bank, $1B to $10B

To **protect against cyberthreats and data breaches** among other benefits.
Credit Union, Less than $1B

Remove some risk prior to signing a new vendor.
Insurance, 5001+ employees

Compliance to federal and state regulation, ensure standardization across organization for vendor selection and requirements and ongoing monitoring.
Bank, $1B to $10B

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

Minimize risk.
Fintech, 501-1000 employees

Costs control and compliance.
Bank, $1B to $10B

Satisfies auditors.
Credit Union, Less than $1B

Compliance and security.
Bank, $10B+

Management of vendor risk and a **way to gauge and measure SLAs to find competitive, low-risk vendors.**
Mortgage, 501-1000 employees

Reduces the risk of third parties who are performing certain functions for or providing services to the bank.
Bank, $1B to $10B

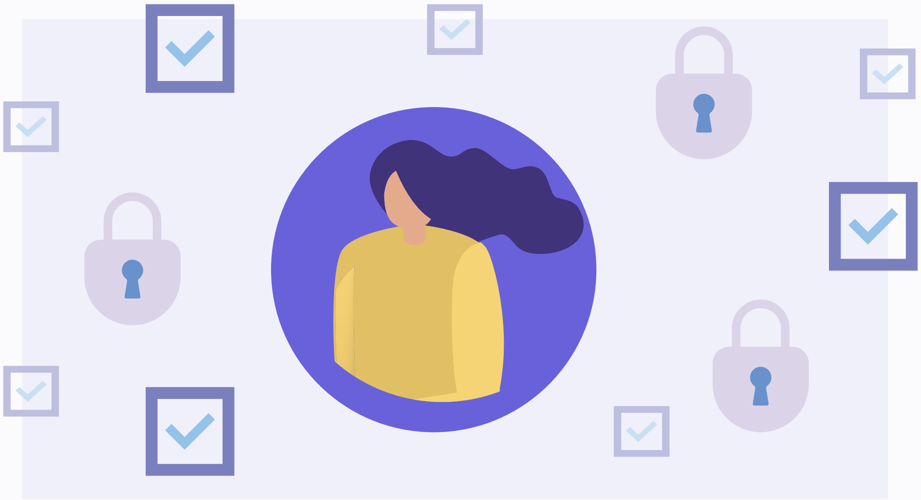
Credibility with clients and regulatory compliance.
Fintech, 1001-5000 employees

Oversight and **transparency.**
Bank, $1B to $10B

Increase **operational and financial efficiencies.**
Wealth/Asset Management, 1-100 employees

Building relationships with knowledgeable and needed vendors while reducing risk.
Bank, $1B to $10B

Clear **depiction of where risk is at.**
Fintech, 101-250 employees



Accurate measurement of risk so we can determine our risk appetite and wrap contractual language around these known risks.
Healthcare, 1001-5000 employees

Keeps examiners/auditors happy; helps the credit union run more efficiently; minimizes risk to our institution and improves security for our organization and our members.
Credit Union, $1B to $10B

Risk tolerance. We know who our vendors are and how they perform.
Bank, $1B to $10B

Helps management **limit the risk of third-party vendors** working with our company.
Credit Union, $1B to $10B

Information security and compliance with regulatory requirements.
Credit Union, $1B to $10B

Making good choices in which vendors to do business with.
Bank, Less than $1B

Attention to the details of who we work with.
Credit Union, Less than $1B

Manage risk.
Fintech, 1-100 employees

Protects our supply chain and ensures we are working with reputable vendors. Helps with compliance with government contracting regulations.
Aerospace, 5001+ employees

Structured and formalized process in risk management and contracting process. Ongoing due diligence and **educating contract owners** regarding their options or what to negotiate for.
Bank, $10B+

Security of the vendors, along with regulatory compliance.
Bank, $1B to $10B

Compliance with regulatory guidance and mitigating risks to fall within the enterprise risk appetite.
Bank, $10B+

Speed and trust.
Bank, $1B to $10B

Knowing when contracts are expiring allows for **negotiations to occur when needed and not at the last minute.**
Education, 1001-5000 employees

Keeps examiners off my back.
Credit Union, Less than $1B

Risk mitigation and compliance with applicable regulations within the industry.
Wealth/Asset Management, 1001-5000 employees

Keeps us aware of vendor activity and meets examination requirements.
Credit Union, Less than $1B

Keep the examiners happy.
Bank, Less than $1B

Cost savings; reputational protection; regulatory protection; customer satisfaction.
Insurance, 1001-5000 employees

Risk mitigation, compliance to regulations.
Bank, $10B+

Identification of risk and control.
Bank, $1B to $10B

Business continuity — **we know if a vendor is going under.**
Bank, Less than $1B

Compliance with regulatory and client mandated reviews.
Wealth/Asset Management, 101-250 employees

Operation cost control.
Credit Union, $1B to $10B

Mitigates risks, cost savings, ensures we look before we leap into new agreements and **ongoing review of third parties allows us to understand risk portfolio and tolerances.**
Insurance, 1001-5000 employees

Risk mitigation.
Credit Union, $1B to $10B

Contract tracking and risk assessments.
Bank, Less than $1B

Cost reduction, risk management and reduction and alignment with compliance requirements.
Insurance, 1001-5000 employees

Risk management.
Consulting, 501-1000 employees

Awareness of our service providers' security controls; contract management.
Bank, $1B to $10B

Reputation protection.
Retail, 1001-5000 employees

Better risk management of vendor relationships regulatory compliance.
Bank, $10B+

Minimizing risk to the institution. Maintaining regulatory compliance. Ensuring vendor performance.
Bank, Less than $1B

May prevent us from signing up to work with a vendor who is not in a good position. **Thorough contract reviews are key to protecting the bank.**
Bank, Less than $1B

Awareness of what our vendors are doing with our customer's information. SLA monitoring.
Bank, $1B to $10B

Keeping in check with regulatory requirements; **being able to spot potential risks before they happen;** provides awareness of vendor risks to executive management and the Board.
Bank, $1B to $10B

Overall protection to the bank.
Bank, $1B to $10B

Effective risk management and **maintain regulatory expectations.**
Bank, $10B+

Vetting vendors, **enhancing security.**
Bank, Less than $1B

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

Organization of contracts into one central location.
Bank, Less than $1B

Monitoring of our third-party vendors.
Bank, Less than $1B

Besides regulatory compliance, it allows us to monitor vendors and their activities and results.
Credit Union, $1B to $10B

Ensuring **customer data is protected** and vendors are performing as expected.
Bank, $10B+

Risk avoidance.
Bank, $10B+

Circumvent specific risk associated with vendor product and or service.
Bank, $10B+

Allows insight into the risks posed by different vendors and potential ways to mitigate said risks.
Bank, $1B to $10B

Measure ongoing vendor performance.
Bank, $10B+

Contract management - **ensuring proper value obtained from vendor** relationships.
Bank, $1B to $10B

It gives us the ability to make better decisions when renewing (or seeking) a third-party relationship.
Bank, Less than $1B

Compliance with regulatory requirements. Structured review with SME provides occasional End-User-Compensating-Control adjustments.
Bank, $10B+

Exam scrutiny.
Credit Union, Less than $1B

Protecting the Credit Union, members and employees from risk exposure. **Ability to streamline and capitalize on vendors** who have scope to serve in other areas.
Credit Union, $10B+

Stability, continuity and risk management.
Lender, 1001-5000 employees

Allows us to **protect our relationships with our clients,** particularly in the realm of data privacy.
Fintech, 1-100 employees

Protects us from potential risks of using a third party, financial risks and regulatory issues.
Credit Union, $1B to $10B

Meet **regulations.**
Insurance, 5001+ employees

Centralized visibility and maintenance of contracts, schedule of automated reviews/ due diligence prompts.
Insurance, 1001-5000 employees

Additional protection of sensitive data. Contract renewal awareness/contract terms protection. **Regulatory compliance.**
Bank, $1B to $10B

Proactive risk management, cost savings, compliance with regulators.
Credit Union, $1B to $10B

Protecting our **customer's data.**
Insurance, 5001+ employee

Safeguarding the organization, it's members and employees **against risk.**
Credit Union, $1B to $10B

Risk management and contract **centralized review.**
Bank, 10B+

Eliminates or at least **mitigates risk** in many areas such as data breach, reputation, etc.
Insurance, 1001-5000 employees

Better oversight of risks related to mission critical suppliers and vendors as well as risks to IT security.
Education, 5001+ employees

Protection.
Bank, $10B+

Avoidance of unacceptable risks to the organization, comply with regulatory compliance and helps business meet objectives.
Insurance, 1001-5000 employees

Assists in **determining where our risk lies** and how we mitigate that risk.
Credit Union, $1B to $10B

Strategic tools for planning and decision making.
Bank, $1B to $10B

Recommendations & Best Practices

Insights from working with hundreds of clients

2020 was a year that 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 our ear to the streets and understanding what our industry is experiencing is certainly indicative of what the road might lead to for us.

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 2021

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

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 almost 1000 clients 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, clients 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.**

(270) 506-5140 | 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 library. The assessments enable clients 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.