

State of Third-Party Risk Management 2020



TABLE OF CONTENTS

03 | About the Survey

04 | A Note from Venminder's Chief Risk Officer

05 | Survey Highlights

06 | Survey Results

07 | Commitment to Vendor Management

07 | Internal Resources Committed to Vendor Management

10 | Primary Reasons

11 | Organizational Structure

13 | Sponsorship from the Top

14 | Vendor Management Processes

14 | Size and Makeup of Vendor Landscape

16 | Technology Tools Used

18 | Best Practices in Vendor Management

19 | Operating Models

20 | State of Third-Party Risk Management

20 | Maturity of Vendor Management Programs

23 | Exam Results

24 | Vendor Management Challenges

25 | Recommendations & Best Practices

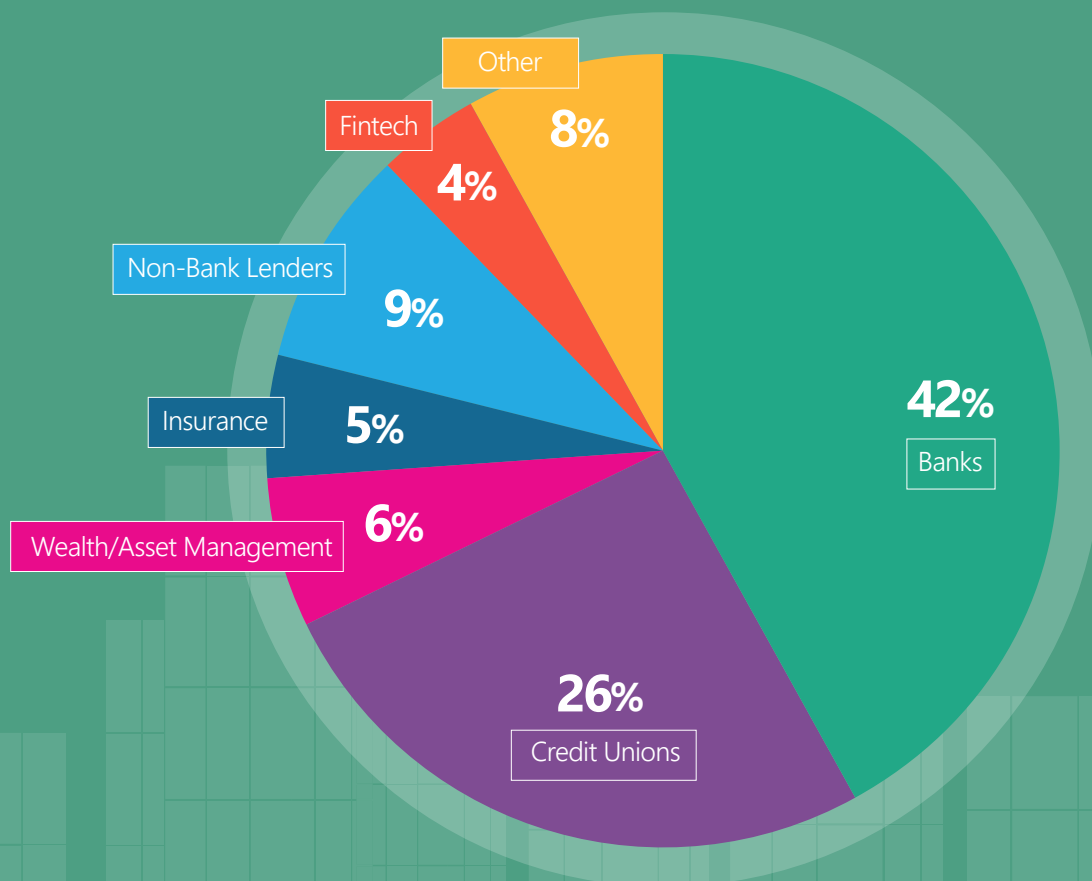
27 | About Venminder

ABOUT THE SURVEY

Venminder's State of Third-Party Risk Management 2020 Survey provides insight into how organizations manage third-party risk in today's increasing regulatory and risky climate.

This is Venminder's fourth annual whitepaper. This year's survey included respondents from a wide variety of different organizations across multiple industries. We believe this year's results provide a broader lens to look at the third-party risk management industry as a whole and, on balance, acknowledge the shared challenges of managing a highly outsourced vendor model.

Venminder promoted the survey to both customers and non-customers through email and social media. Results were tabulated as of December 17, 2019. To increase confidence in the validity of responses, answers are anonymous.



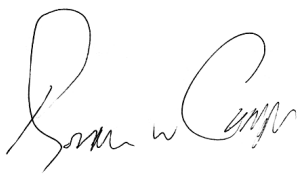
A NOTE FROM VENMINDER'S CHIEF RISK OFFICER

Thank you to everyone who participated in our fourth annual state of third-party risk management industry survey. This year's survey included our largest response yet and cut across several industries so we believe it provides terrific insight into the challenges of doing third-party risk management well in today's ever-changing environment.

I think we were all surprised to see very little new guidance coming out in 2019, and with the 2020 election looming, that's not likely to change. If there's any good news in that, it allows us to get really good at what we know how to do and do it well.

The changes in privacy standards and cybersecurity will dominate headlines, I am certain, as will the continued fight over the Office of the Comptroller of the Currency's (OCC) proposed fintech charter. "2020" is often a term associated with having great vision – the 2020 survey has given us great vision into where industries are headed – the regulatory expectations are certainly not decreasing. More importantly, doing third-party risk management well helps protect all of us from data breaches, bad actors and rogue vendors.

So, without further ado, let's see what you all had to say and, again, thank you for participating!



Branan Cooper

Chief Risk Officer

branan.cooper@venminder.com

SURVEY HIGHLIGHTS

Venminder's State of Third-Party Risk Management 2020 Survey included respondents that represent a wide variety of organizations across multiple industries. The perspectives of additional organizations outside of the heavily regulated financial services industry allows us to learn more from each other and share best practices across the entire spectrum.



Continued limited spend outside of FTE cost, barely enough to do a single on-site visit



Effective vendor management creates a real return on investment while heading off problems



The majority of respondents are doing things "correctly" overall



Majority of respondents (72%) have 1-5 people in vendor risk management



There continues to be a migration to make third-party risk independent of lines of business and report to the board or senior management

Survey Results



COMMITMENT TO VENDOR MANAGEMENT

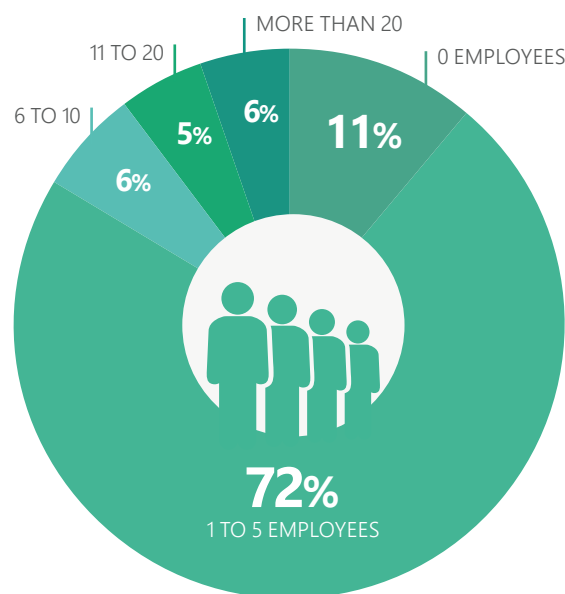
Internal Resources Committed to Vendor Management

Continuing to See Slight Improvement

The trend to having more employees dedicated to a vendor risk management program continues. In 2018, 90% said they have less than 5 employees, in 2019 77% and for 2020 72% said they had 5 or fewer employees. The trend to have more employees continues with 17% now having 6 or more employees dedicated to their vendor risk management program.

Given the challenges of third-party risk management, it's important that the function is appropriately staffed with people sufficiently trained to do the job (whether through in-house or supplementing externally). As we see later in this document, time management and having the right resources are resonating challenges for all, particularly at smaller organizations where vendor management may be an afterthought for the already overwhelmed risk/compliance manager.

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



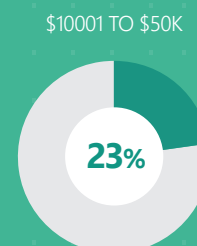
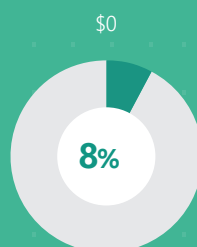
Besides full-time employees cost, how much budget has been dedicated to vendor management?



Interested in a deeper dive?

Download our supplemental report for organization type and size breakdown.

[Click here.](#)



74%

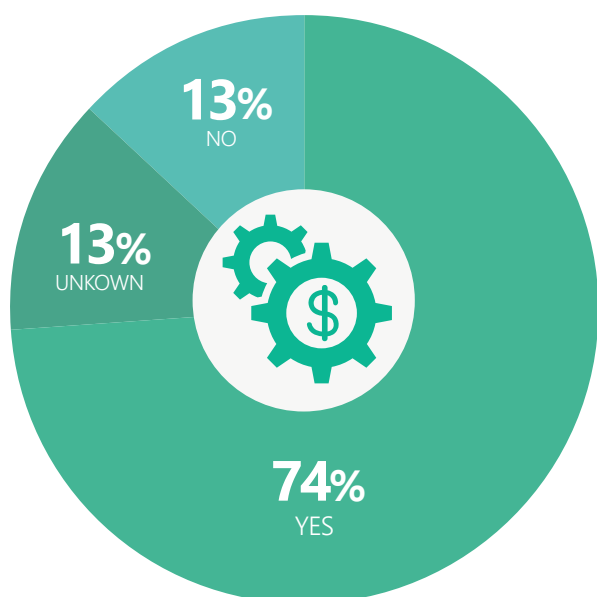
of respondents believe there is a **return on investment (ROI)** from efficient vendor risk management.

Thirty-eight percent (38%) of respondents report spending less than \$10,000 on vendor management, not including direct personnel expenses.

Making the appropriate investment proves to examiners that vendor management isn't just a once a year exercise at exam time, but an ongoing commitment of the organization's resources.

An ounce of prevention is worth a pound of cure, particularly when cleaning up costly breaches, paying large enforcement fines and overspending to shore up a critical function that should be continuously invested in. When you consider how much money your organization spends on its physical appearance, isn't it worth spending at least that much on its compliance, operational and reputational risk? What if you need to visit a vendor for onsite due diligence – that alone would cost more than \$5,000, most likely.

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 is 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, 74% of respondents believe that there's a ROI.

We suggest that those who don't see a link between vendor management and ROI explore how a well-managed program can drive real cost savings by preventing unwanted automatic contract renewals and by performing champion/challenger scenarios to find the most cost-effective vendors. It's very likely these organizations will be surprised at how much they can save. Vendor risk management as a discipline is maturing and the people doing it are starting to realize the benefit, not to mention the cost avoidance of heading off expensive problems before they occur.

The cost of overlooking a contract auto-renewing could cost an organization dearly, we hear time and time again of contracts being lost or alerts not in place and in some cases, a contract auto-renewal costing many millions.

While it's not just about the return on investment, there is real strategic value in doing vendor risk management consistently well.

It's easy to calculate the return in the form of cost avoidance of preventing a costly contract from auto-renewing or comparing vendors for the best cost and quality. It's encouraging to see that 74% do believe vendor risk management as a discipline is maturity and the people doing it are now seeing the benefit of it in dollars and cents.

To help obtain management's buy-in for vendor management, we recommend that you do two things. First, add up all the cost of your contracts with vendors and take a look at the increases in costs with each annual renewal. That's the hard dollar volume your company is managing each year. We find that typically, an organization will add 2.5% to their bottom line if they are managing their vendors properly. Research your company's history then talk to management about any history of auto-renewing and discuss that 2.5% increase in the bottom line. We highly recommend that the third-party risk department should maintain a list of contracts that auto-renew and mark any that automatically renewed in error.

72%

of respondents have
between 1 to 5 employees
dedicated to their vendor
management program.



Primary Benefits

We asked this year's respondents to provide what they believe are the primary benefits of vendor risk management. We've highlighted the answers below, removing the duplicates. It's clear, vendor risk management has many benefits.

What do you believe are the primary benefits vendor risk management gives your organization?

VISIBILITY OF POTENTIAL RISKS
MAKE RISK AWARE DECISIONS **MITIGATING RISK**
PREPARED QUICKLY REACT TO CONCERNS OR ISSUES
CONTROL OVER EXPOSURE
OVERSIGHT OF DELIVERY OF SERVICES IDENTIFY POTENTIAL RISKS
COST EFFICIENCY **CONTROL COSTS**
OVERSIGHT OF CONTRACTUAL OBLIGATIONS PROACTIVE PROTECTION
ACCOUNTABILITY PROTECTION TO SHAREHOLDERS
STANDARDIZING VENDOR ACCOUNTABILITY CENTRAL LOCATION FOR CONTRACTS
LINE OF SIGHT STAYING ABREAST **LEVERAGE**
SAFEGUARD CUSTOMER INFORMATION FIND CONTRACTS
AVOIDING PENALTIES REDUCE POTENTIAL FOR BUSINESS DISRUPTION
AVOIDING POTENTIAL NEW BUSINESS LOSS STRONGER RELATIONSHIPS
COMPLIANCE COST SAVINGS THROUGH NEGOTIATIONS
PROACTIVE CONTROL OF VENDORS
CONTROL OF INFORMATION FINANCIAL STABILITY SATISFYING REGULATORS
KNOW THE VENDOR IS FOLLOWING REGULATIONS **BETTER INSIGHT**
AVOID NON-PERFORMING VENDORS
AWARENESS KNOW WHO YOU ARE DOING BUSINESS WITH
CONTROL RISK OF EXPOSURE TO DATA BREACHES
QUALITY OF WORK SECURITY AND ASSURANCE REPUTATION PROTECTION
TRANSPARENCY **TRUST BUT VERIFY**
BETTER PREPARATION FOR AUDITS UNDERSTANDING OF VULNERABILITIES
AVOID AUTO RENEWALS REGULATORY PROTECTION SINGLE REPOSITORY
ENSURE VENDORS MEET OR EXCEED STANDARDS PLANS FOR THE UNEXPECTED
AVOID DUPLICATING EFFORTS IMPROVE QUALITY OF SERVICES
ONE-STOP SHOP FOR VENDOR COMPLIANCE
FINDING GAPS IN THIRD AND FOURTH PARTIES ENSURE WORKING WITH REPUTABLE BUSINESSES

Primary Reasons

Regulatory requirements remain dominant

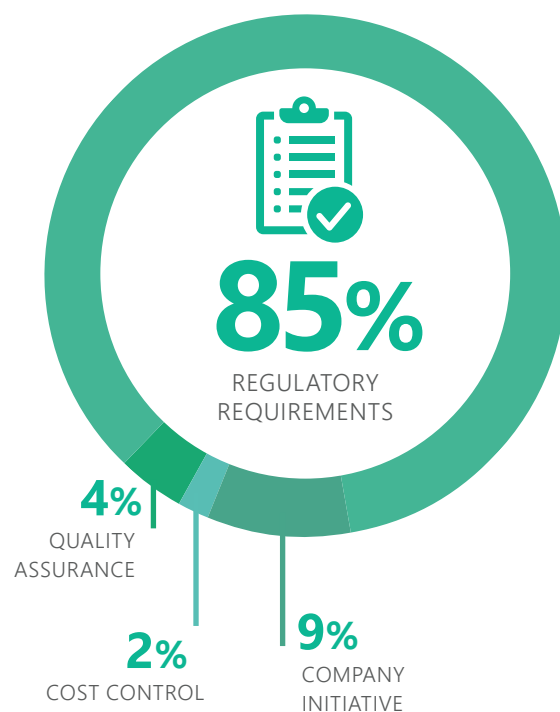
Not surprisingly, the regulatory requirements pretty much dictate the need for vendor risk management, though it's encouraging to see a nod toward quality assurance, which is where many vendor management programs got their start many years ago. We still believe, as we saw earlier, there's a real cost control component that should be further explored.

Organizational Structure

Independence from lines of business continues

As organizations grow and mature, and as regulators issue guidance on active board involvement, third-party risk management practices must evolve. The best practice and industry de facto standard is to have third-party risk management independent from the lines of business and back office functions. It's critical that third-party risk management assert its independence from the lines of business to prevent business priorities from overriding vendor risk concerns.

What is your primary reason for doing vendor risk management?



85%

of respondents say **regulatory requirements are their primary reason** for doing vendor risk management.



Fifty-one percent (51%) surveyed say that they report to the senior management team or committee of the board.

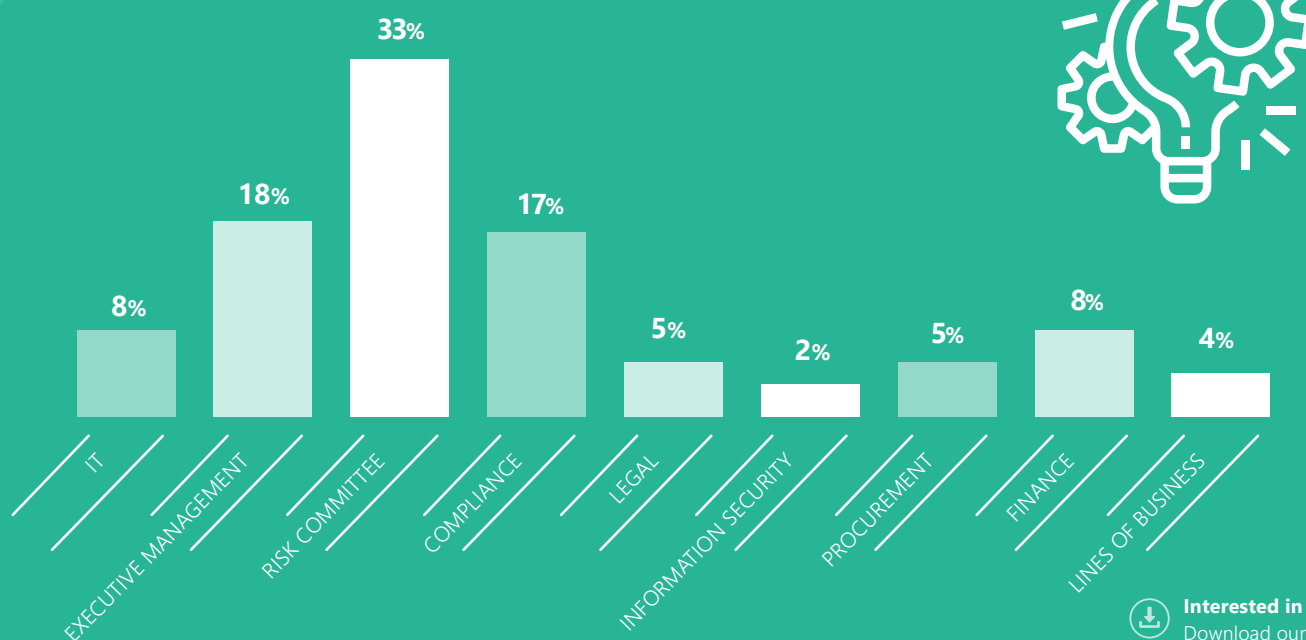
It's concerning that there are still some third-party risk programs still reporting to IT or Information Security. The reason this is concerning is that their primary focus should be on the technology and how they're going to support the strategic initiatives of the business. When third-party risk is put in a technical group, issues will typically arise as IT can be swayed by favorite vendors, cost considerations or ease of implementation rather than risk.

Four percent (4%) indicated reporting to lines of business. This is common through a decentralized program but also comes with its own challenges. Typically, someone in a line of business is going to put their self-interest ahead of the organization's and that poses a real danger of overlooking key elements of risk. They may or may not negotiate to the level someone else would. Also, deadlines could be missed. Their primary objective is their position.

However, giving the business units a voice in third-party risk is important so the business can't ignore risk management implications when outsourcing a key product or service.

Elevating vendor risk management to an enterprise level/risk committee reporting structure helps create transparency throughout the organization's stakeholder base and that transparency needs to extend to anyone who should be at least aware of the details as to what vendors to partner with and what contracts should be in place. Certainly, the regulatory guidance stresses the need for active board involvement, so tying it to an executive team or risk committee helps accomplish that objective.

Where does vendor management report?



Interested in a deeper dive?

Download our supplemental report for organization type and size breakdown.

Click here.

Sponsorship from the Top

Setting the tone from the top is important

Fourteen percent (14%) find securing business unit support challenging with 69% saying that it's challenging but they're managing. It's incredibly important that senior management takes vendor management seriously and is willing to stand behind the vendor management team or compliance officer when key decisions need to be made – whether it's escalating a due diligence request, following up on a discussion to terminate a vendor or simply not changing direction without involving the vendor management team.

We're seeing a trend towards employee awareness programs through the companies where vendor managers are implementing initiatives to train and educate everyone, from management to the lines of business, about the importance of communication and working together to minimize vendor risk. This is **key for 2020**. Everyone needs to be on the same team and to understand "why" third-party risk management is so important and how it can impact the bottom line. If employees understand how they "fit" into the big picture, they'll be more open to participate.

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



69%

of respondents **say it is challenging but manageable to secure business unit support** for their vendor management program requirements.

VENDOR MANAGEMENT PROCESSES

Size and Makeup of Vendor Landscape

At most organizations, vendor management is complex

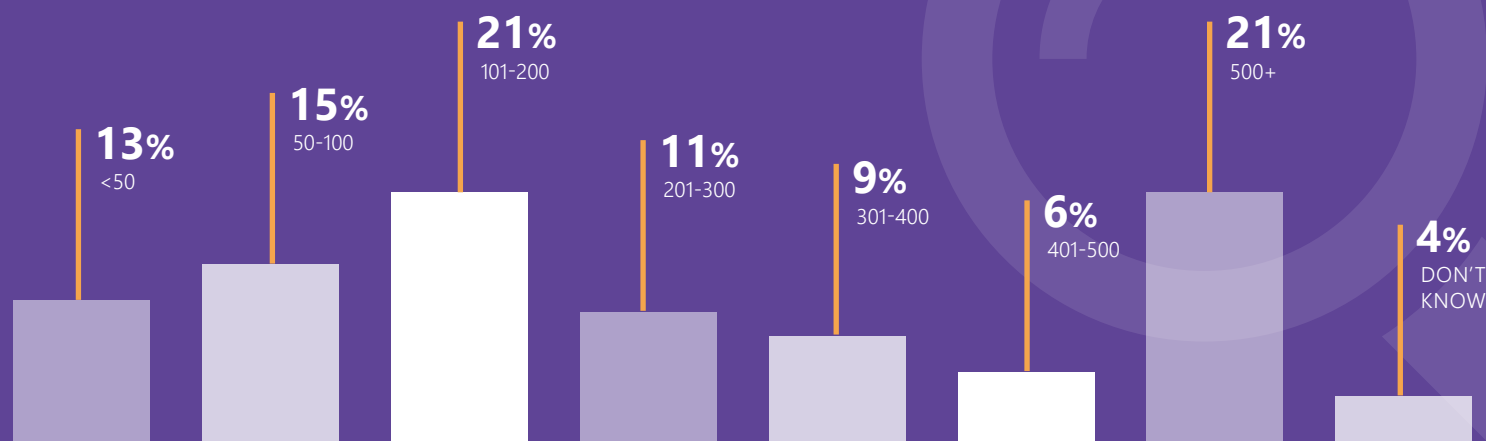
With so much pressure on margins and more customers in today's competitive landscape, one way to cut costs is to outsource functions. However, organizations must actively manage those outsourced activities. A greater reliance on outsourcing has an exponential impact on the amount of time and resources needed to ensure that outsourced products and services are consistent with the organization's appetite for risk.

We encourage customers to verify that descriptions of actively managed vendors are up-to-date, accurate and identify which vendors are in scope and out of scope. Not every vendor needs to be actively managed – such as the Staples supply order, the person who delivers pizzas to your team's luncheon and the car rental agency used in business travel – but take a risk-based approach and apply all the tenets of third-party risk management, to the extent reasonably practical, to those that are actively managed.

21%
of respondents report that
they have more than
500
vendors included in their vendor
management programs.



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



Interested in a deeper dive?

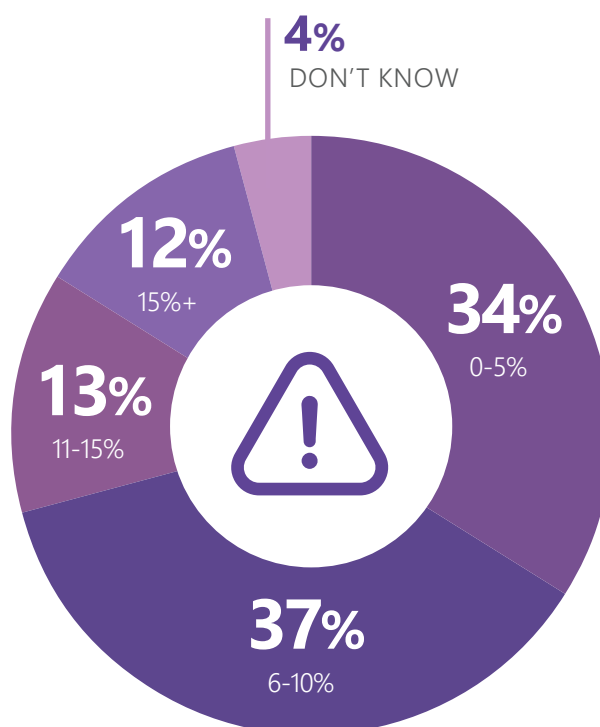
Download our supplemental report for organization type and size breakdown. [Click here.](#)

A standard measurement is that organizations typically classify about 10% of their vendors as critical. These results don't change much from year-to-year, indicating that organizations have a strong handle on the vendors most impactful to their business.

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.

For those 12% who report that more than 15% of their vendors are critical, we suggest revisiting how many core services are outsourced and how aggressively they need to be managed. The definition of "critical" can sometimes vary but typically there are three questions – **would a sudden loss of this vendor cause a disruption to your organization; would that disruption impact your customers; would the time to recover be greater than one business day or greater than what your organization's business continuity plan calls for as a recovery time?** If any of these are "yes", that's a critical vendor – start thinking about business continuity and exit strategy planning.

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





65%

of respondents indicate that **they use a dedicated vendor management software platform** to manage their vendors.

Technology Tools Used

Marching toward more automated solutions

Sixty-five percent (65%) of respondents indicated that they use a dedicated software platform to manage third-party risk, an increase we are seeing year-over-year as many make the move from Excel to a technology platform.

Eleven percent (11%) say that they use a vendor risk management module inside an ERM/GRC platform. These must be carefully reviewed as most ERM/GRC platforms are built to manage risk vs. having a strong vendor risk management program. Normally, they require a heavy upfront investment in getting the ERM/GRC system “tweaked” to handle vendor management. Unfortunately, outdated customizations tend to plague these vendor management programs. The level of detail that a program needs today is extensive!

We recommend that those 18% still using Excel or database for vendor management begin actively capturing the time they spend on maintenance of the system they have in place. It’ll probably startle you. While they appear to be inexpensive options, people end up spending the majority of their time trying to open multiple spreadsheets, each with multiple tabs, just to update a single data element. It’s time-consuming and very error prone and only serves to further tax limited resources.

What is your primary tool for managing your vendors?

15%

EXCEL

3%

ACCESS
DATABASE

65%

A DEDICATED VENDOR
MANAGEMENT
SOFTWARE PLATFORM

11%

A VENDOR MANAGEMENT
MODULE INSIDE OF AN
ERM PLATFORM OR GRC

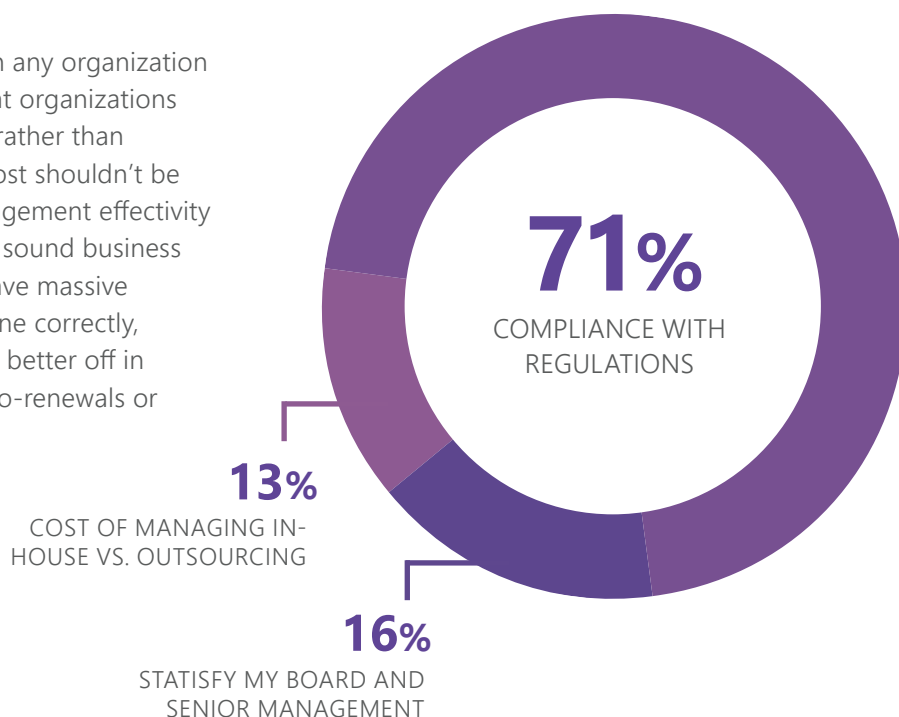
6%

OTHER

Nearly consistent with last year, compliance is the primary focus. Regulatory compliance is the number one consideration for over 70% of respondents when considering a compliance or risk solution.

Cost isn't a prevailing consideration in any organization type which is an encouraging sign that organizations are managing risks and expectations rather than cost. However, we recommend that cost shouldn't be discounted as to do vendor risk management effectivity today, a technology solution is now a sound business practice and can have an impact to save massive dollars. With vendor management done correctly, organizations will surely be financially better off in the long run by avoiding contract auto-renewals or inappropriate vendors.

In considering compliance or risk solutions, what is your primary goal?



71%

of respondents consider **compliance with regulations as their primary goal** when considering compliance or risk solutions.



Do you require a written or formal risk assessment for all new vendors pre-contract?



29%
NO

71%
YES



Interested in a deeper dive?

Download our supplemental report for organization type and size breakdown. [Click here.](#)

Best Practices in Vendor Management

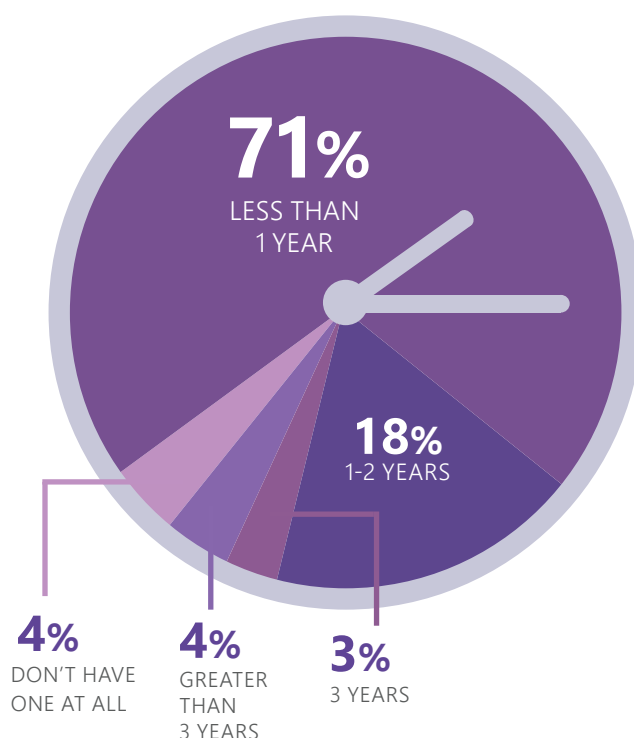
Several tried and true methods continue to stand the test of time

Seventy-one percent (71%) of respondents require a pre-contract risk assessment. The pre-contract risk assessment is not only a best practice and general industry standard, but informs management of the risks they're assuming, allows them to craft better contracts to address risk and highlights additional areas for due diligence and ongoing monitoring. Once the contract is signed and the vendor is onboarded, it's more difficult to establish appropriate reporting, breach notification provisions, obtain missing due diligence and a myriad of other items. It's not just a good idea, it simply better helps inform the due diligence, contract and oversight processes.

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 71% updating their vendor management policy annually.

Just like an annual checkup that can catch a medical issue early, the longer you leave the vendor management policy in place without refreshing it, the longer a potential unseen concern can grow and get worse. Keeping the board informed and engaged is important as well, and an annual refresh of the policy, much like other compliance and risk policies that are updated annually, is a great way to accomplish that.

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



Of concern is that 4% of organizations that do not have a policy at all. Vendor management requires structure and discipline and regulated organizations need to prove to regulators that they've read and understand the guidance. A written policy accomplishes that goal.

Maybe it's just a hiccup, but seeing that the industry has slipped a bit from year-to-year is concerning in terms of keeping their policies updated each year.

Operating Models

More than half of respondents have a centralized model

Over half of respondents are using a centralized model where usually the lines of business interactions are being managed through the vendor management department/person. Generally, in this model, the vendor risk management department/person is partnered with the lines of business to ask the hard questions and work through them with a research/collaborative approach.

A third of respondents use the hybrid model, where most of their vendor management is likely centralized (i.e., contracts and reporting) but they're still using the lines of business for some functions (e.g., monitoring service level agreements (SLAs) and adhering to contracts). Larger and more complex organizations with vastly different business unit functions often need to rely on a hybrid approach as it can be nearly impossible to set standards that'll work for the entire organization. This is especially true if the organization is deliberately keeping third-party risk group staffing low. It's important with this model that each party's role and responsibilities are clear to avoid gaps or wasteful overlaps.

Seven percent (7%) are using a decentralized model which can be difficult. It means that the responsibilities to manage the risk the vendors pose are on the lines of business. While it's certainly better than not having a program, it's impossible to get everyone to participate at the same level.



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



Interested in a deeper dive?

Download our supplemental report for organization type and size breakdown.

Click here.

6%
TOTALLY
OUTSOURCED

33%
HYBRID

54%
CENTRALIZED

7%
DECENTRALIZED

STATE OF THIRD-PARTY RISK MANAGEMENT

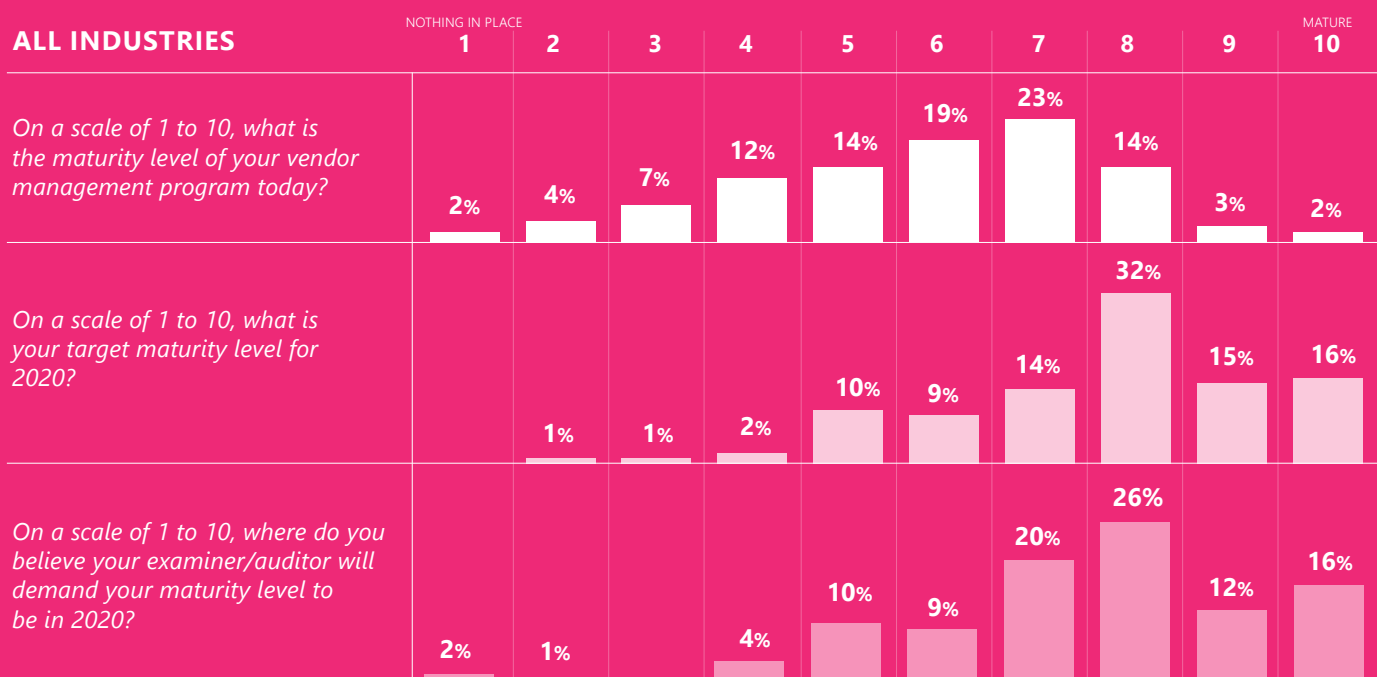
Maturity of Vendor Management Programs

The trend towards program maturity continues

We asked respondents to rate their current program maturity level, their target level and where they believe regulators expect them to be on the maturity scale. As in previous years, survey respondents continue to aspire to a more mature vendor management program. Respondents show that they're concerned about heightened expectations and regulatory requirements yet express an eagerness to evolve toward greater maturity in their processes.

Non-bank lenders also express the need to make a big leap from their current levels to where they believe their target maturity should be.

We asked respondents to number on a scale of 1 to 10, what the maturity level of their vendor management is today, what their target maturity level is for 2020 and where they believe the examiners/auditors will demand the maturity level to be at in 2020.

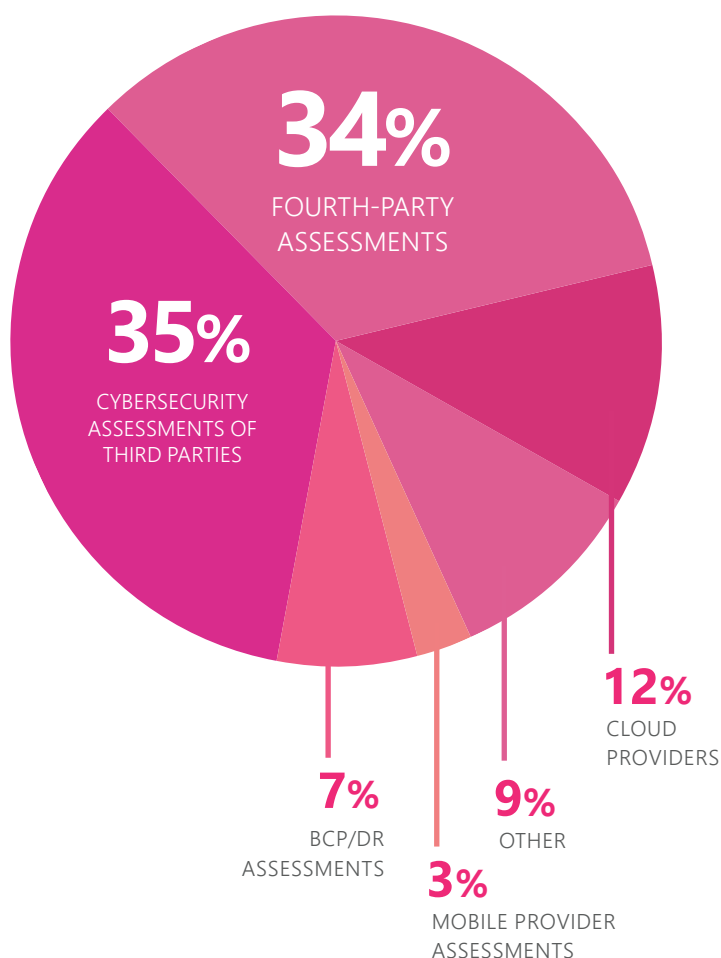


Credit unions and banks have the highest expectations from a regulatory perspective, anticipating that their regulators require them to have the greatest level of maturity. This makes sense: the National Credit Union Association's (NCUA) current guidance dates all the way back to 2007. Think about how much technology, such as mobile banking and remote deposit capture, have changed in the past 13 years. The guidance hasn't changed but regulators expect that credit unions are further along on the maturity scale since they've had more than a decade to develop their vendor management programs.

Federal Deposit Insurance Corporation (FDIC) and OCC regulated organizations have also experienced a steady drumbeat of guidance in the form of FDIC FIL's 44-2008 and 3-2012, followed by the OCC Bulletins 2013-29, 2017-7 and 2017-21, all glued together by the regular updates to the Federal Financial Institutions Examination Council (FFIEC) IT examination handbook.

Fintechs will need a "bank-like" level of maturity in third-party risk management processes alongside any other consumer protection regulations, regulatory guidance and applicable laws, depending on their products or services.

What do you see as your next biggest hurdle?

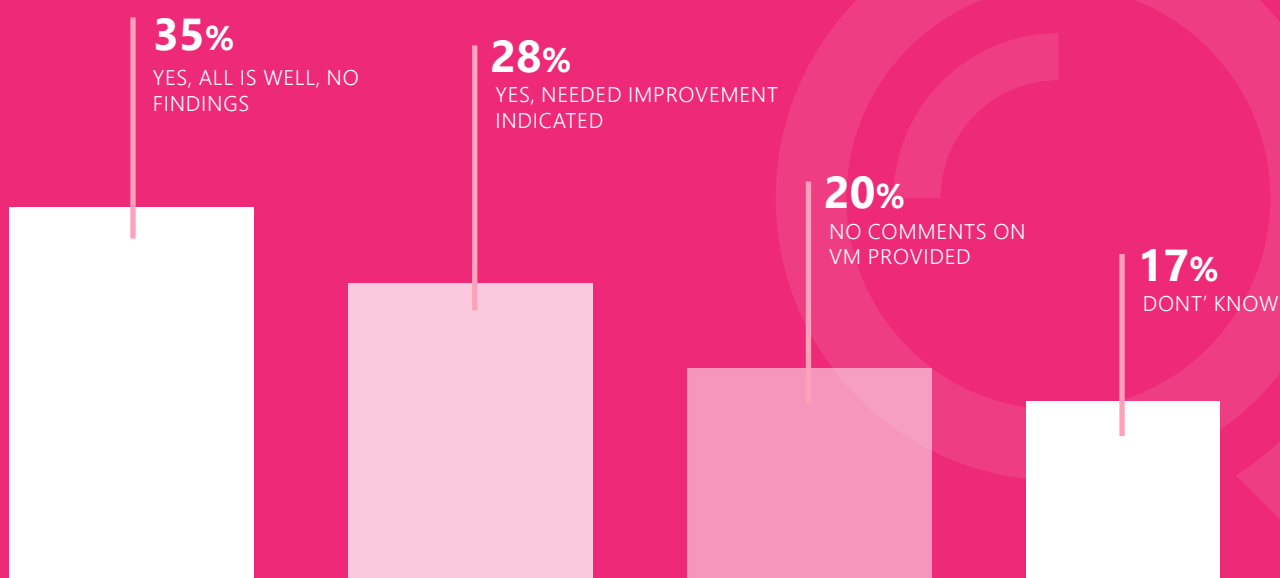


Thirty-five percent (35%) of respondents say that cybersecurity assessments are their next biggest hurdle. Today, data protection laws and their applicability to organizations are growing rapidly. California's Consumer Privacy Act (CCPA) quickly followed the European Union's General Data Protection Regulation (EU GDPR) and many other US states are preparing their own data protection laws. These new laws have many similarities including ensuring vendors have certain privacy capabilities and can demonstrate "reasonable" or "appropriate" internal security controls. It's important organizations show whether those capabilities are present and how information is being secured. The complexity of managing multiple states' and multiple countries' varied regulations will be challenging.

It appears from last year to this year, many in the industry worked to educate themselves on fourth-party assessments. Forty percent (40%) last year said it's the biggest hurdle. Thirty-four percent (34%) this year said it's the biggest hurdle – a decline by 6%. Fourth-party assessments go hand-in-hand with data protection. While there has been very little mention in formal guidance regarding fourth parties, examiners and auditors are laser-focused on organizations that have even tangential access to customer data and what the third party is doing to protect it.

Today, organizations must be able to ensure that whomever has their data can meet CCPA requirements. Typically, we see contracts with the right to audit clause, however, most rarely exercise it. It's important that there's an agreement in place that the vendor will destroy the data after termination. Remember, data diagrams can be viewed to see the data trail. It's also important to contract with vendors to get them to assure you that they meet CCPA requirements and they indemnify you from any lawsuits from a result of not meeting CCPA . While you can't ever give away your responsibilities, contract language can be placed to help protect you.

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



Interested in a deeper dive?

Download our supplemental report for organization type and size breakdown. [Click here.](#)

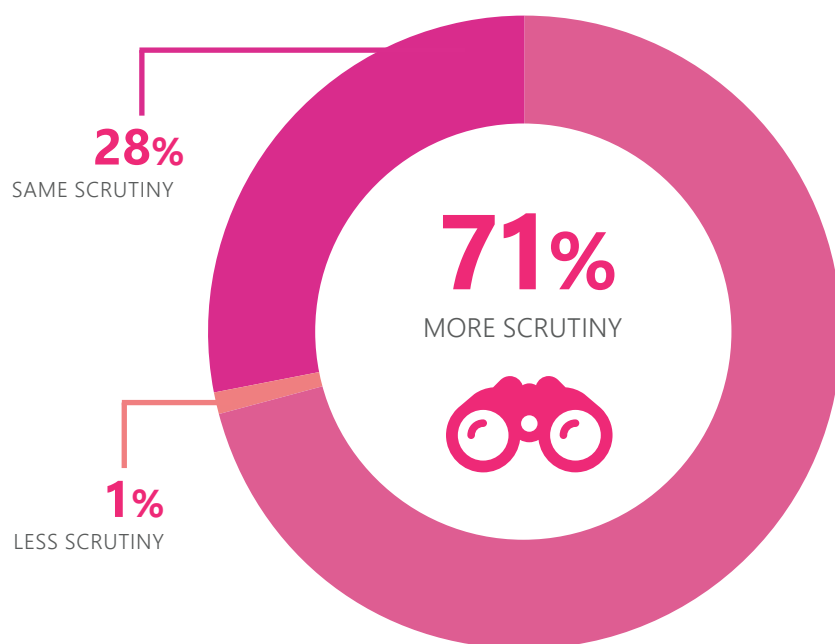
Exam Results

Signs of increased regulatory focus on vendor management

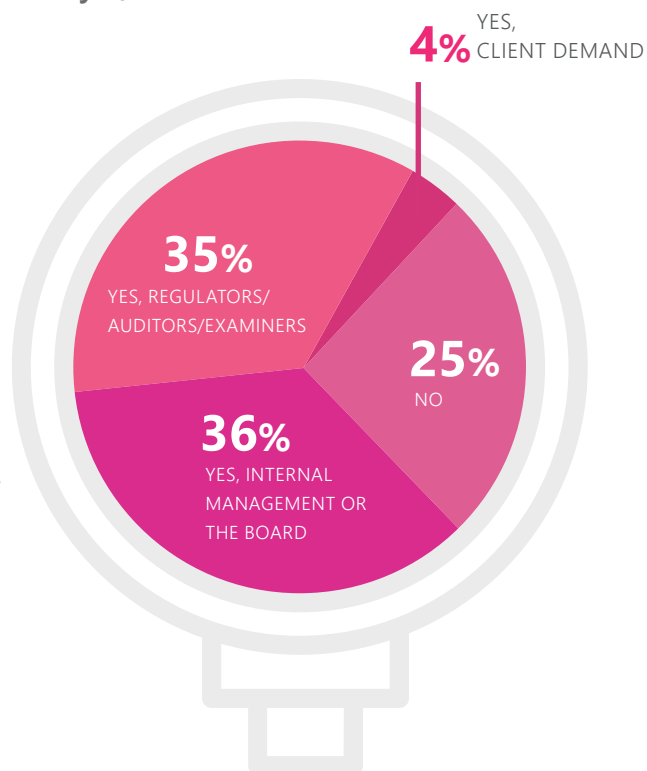
There's been a noticeable jump in programs needing improvement – 23% last year versus 28% this year. It's an indication and confirmation that regulatory relief isn't on the horizon like anticipated in prior years. With so much focus on cybersecurity and vendor management, there'll only be more focus on the risks associated with outsourcing key processes.

Three quarters of respondents feel pressure to improve third-party risk management from either the regulators, internal management/board or customers. The drive from the top down will continue to drive the maturity of the third-party risk management industry. Even though the Consumer Financial Protection Bureau (CFPB) and other regulators have focused on enforcing alternative items, third-party risk is never far from the front burner – your board and senior management must stay actively involved and, while that keeps pressure on the vendor management team, it's an important series of ongoing conversations.

From your perspective, is third-party risk management getting more scrutiny or less scrutiny by the regulators?



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



This survey result should come as a shock to no one: only 1% of respondents believe that third-party risk is getting less attention from the regulators while the overwhelming majority (71%) feel it's getting more attention and 28% believe it has stayed the same.

From our perspective, we absolutely see the regulators from all industries paying more attention to third-party risk. There were multiple newsworthy and notable actions throughout the year that have defined third-party risk. We anticipate that regulatory scrutiny is going to be actionable with negative consequences if an organization isn't following guidance and a third party of theirs is breached.

Vendor Management Challenges

Getting the right documents is still an issue

For the third year, gathering documents from vendors continues to be one of the biggest of vendor management challenges. It's time-consuming and all too often requires a lot of chasing and reminders to receive the documents. However, it's absolutely required. Most in a vendor risk role will speak to being faulted by examiners/auditors for not getting the right documents, so the pressure is intense. Without the right documents, it's not possible to analyze and assess vendor risk. We recommend that it's written in your contract with the third party exactly what documents they'll provide you and when. This will make the task a little easier. Alternatively, you can outsource document collection chasing to a third party.

What are your top 3 vendor management challenges today?



Interested in a deeper dive?

Download our supplemental report for organization type and size breakdown. [Click here.](#)

RECOMMENDATIONS & BEST PRACTICES

Insights from working with hundreds of customers

If creating or refreshing your vendor management program hasn't been high on your priority list, move it up the list right away. Vendor risk management must be an annual and "as needed" exercise that includes getting approval from the board and senior management. For those organizations that have staffed a third-party risk management function, examine the adequacy of resources and investment dollars devoted to the program and consider adopting a more centralized approach.

Board and senior management involvement is a must (and in most cases, regulatory required) so make creating meaningful board-level reporting and capturing those results in minutes of senior management meetings a priority.

Finally, with the intense focus on cybersecurity and increased expectations around the role that fourth parties play, the working relationship between your organization's vendor management program and information security requires ongoing development. Keep that in mind as you ramp up your program in 2020.

THE 7 PILLARS OF VENDOR MANAGEMENT

Incorporating the seven pillars into your vendor management program will provide big microchanges for your organization.

Here are some tips to implement during each pillar stage:

Vendor Selection

- Work with your line of business to gather the top five requirements for any new product or service.
- Remember, there's never just one right vendor so multiple vendors should be evaluated.

Here are 10 best practices for 2020.

Ensure your organization:

- 1 Has a well-documented policy, program and procedures
- 2 Deploys a rigorous set of practices that address each pillar of third-party risk management
- 3 Has adequate credentialed staffing
- 4 Works to foster a supportive board and senior management team
- 5 Includes third-party risk management in annual policy updates and internal audits
- 6 Invests in education, staffing and tools
- 7 Regularly reviews regulatory guidance, legal analysis and enforcement actions
- 8 Periodically, and at least annually, updates all documents and practices
- 9 Adequately and effectively performs ongoing monitoring and follows up on deficiencies
- 10 Keeps a close watch on customer complaints as they're often the fodder for enforcement actions



- Make sure your lines of business are using a champion vs. challenger strategy. Champion vs. challenger is a strategy when you compare vendors and have them “compete” on a level playing field to determine the best quality and service delivery for the expense you’re paying.
- Ask your lines of business if the vendors they’re using are meeting all of their needs.

Risk Assessment

- Review your vendor risk assessment process periodically and look for ways to improve efficiency.
- Ask yourself the question, “Is our risk assessment scale correct?”
- Create a vendor risk assessment schedule that establishes the frequency assessments will be completed or, if you have one, review your risk assessment schedule to ensure it aligns with your strategy.

Due Diligence

- Measure, assess and plan (MAP) your current due diligence process. This stands for the following:
 - **M**easure how many due diligence documents you’ll need to review and how long each one takes.
 - **A**ssess your current due diligence process and look for ways to smooth out the workflow.
 - **P**lan your due diligence strategy for each critical and high-risk vendor. Make sure to include your lines of business.
- Identify any vendors where issues seem present and increase oversight.

Contractual Standards

- Review the standard sections found in the contracts with your legal team and your senior management team.
- Outline your organization’s standard response to each section.

Reporting

- Create a template slide deck that covers each of the seven pillars – one slide dedicated to each one.

Ongoing Monitoring

- Review the SLAs in place for all of your critical and high-risk vendors with your lines of business and determine if they’re adequate.
- Review the key performance indicators (KPIs) in place for all of your critical and high-risk vendors with your lines of business and determine if they’re adequate.

Exit Strategy

- Review the exit strategy you have in place for each critical and high-risk vendor.
- If you don’t have an exit strategy for each critical and high-risk vendor, it’s time to create one.
- Identify at least one potential alternate vendor for each of your critical and high-risk vendors so that you always have a backup.

ABOUT VENMINDER

Venminder offers a world-class SaaS platform that guides and streamlines third-party risk management. Venminder's platform helps users collaborate on all things vendor-related and guides through critical processes such as oversight management, contract management, risk assessments, due diligence requirements, questionnaires, SLA management, vendor onboarding and more. The company has one of the largest libraries of completed assessments available on individual vendor controls that are fulfilled by on-staff industry experts. Venminder also powers Third Party ThinkTank, an online free community dedicated to third-party risk professionals.

STAY UP-TO-DATE WITH VENMINDER

- ✓ Webinars
- ✓ Third Party ThinkTank Community
- ✓ Industry Interviews
- ✓ Videos and Podcasts
- ✓ Third Party Thursday Newsletter
- ✓ Blog

Or, visit the entire Resource Library by **clicking here**.

NEED ASSISTANCE? LEARN ABOUT VENMINDER'S

- ✓ Software
- ✓ Control Assessments
- ✓ Professional Services

FOLLOW US ON

-  LinkedIn
-  Twitter
-  Facebook

DOWNLOAD THE SUPPLEMENTAL REPORT

Interested in a deeper dive of the survey results? **Download the companion supplemental report** that breaks down respondents results by organization type and size.



400 Ring Road, Suite 131
Elizabethtown, KY 42701
(270) 506-5140
www.venminder.com

