venminder

State of Third Party Risk Management 2019

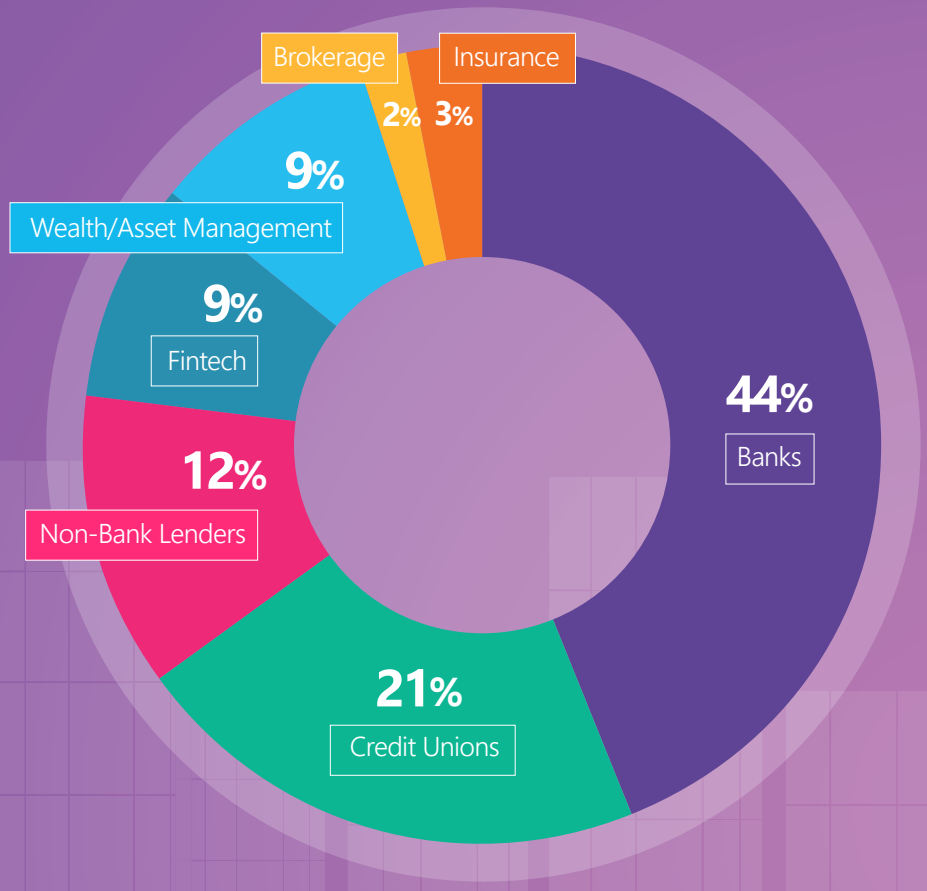
TABLE OF CONTENTS

ABOUT THE SURVEY

Venminder's State of Third Party Risk Management 2019 Survey provides insight into how financial services and financial technology companies manage third party risk management in today's increasing regulatory and risky climate.

This is Venminder's third annual whitepaper. This year we expanded the survey to include respondents from the wider financial services and financial technology 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 clients and non-clients through email and social media. Results were tabulated as of December 17, 2018. 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 third annual state of third party risk management industry survey. I'm pleased to note that we had the highest ever number of responses and from a wider variety of companies.

At the start of 2018, many of us had high hopes for regulatory reform. However, with exception of the reduction in exam cycle frequency for financial institutions under $3 billion in assets, very little reform that directly impacts third party risk managers or gives compliance managers much needed relief has passed. With the continued, unrelenting threat posed by cybersecurity incidents, 2019 is shaping up to be a challenging year. In addition, most of the major regulators have had leadership changes and we're still waiting for the first actions of the new director of the Consumer Financial Protection Bureau (CFPB).

There's quite a lot of change going on, but as the dust settles and new priorities emerge, we as an industry must be prepared for a renewed focus on third party risk. Although I don't like to comment on politics, the shift from a Republican House to a Democratic House will result in leadership changes in some key committees that will inevitably put pressure on regulators to tighten their stance on numerous issues.

I often tell people that I'm now doing the same job I did in banking for many years but without a regulator looking over my shoulder and with the opportunity to help thousands of companies at a time. I hope that the information in this report can help steer you through the churning waters of third party vendor risk management.

Enjoy this whitepaper highlighting our findings and our insights. As always, we welcome any feedback or additional insight you'd like to offer. Here's to a great 2019.

Branan Cooper
Chief Risk Officer
branan.cooper@venminder.com

SURVEY **HIGHLIGHTS**

Venminder's State of Third Party Risk Management 2019 Survey included more than double the respondents from previous years representing a wider variety of companies across the financial services and financial technology industries. The perspectives of additional companies that face the challenges of an incredibly difficult risk management landscape allows us to learn from each other and share best practices across the entire spectrum of the financial services and financial technology industries.

77%

report five or fewer employees dedicated to vendor management.

As in prior years, we were disappointed that the vast majority (77%) of respondents report that they have fewer than five full-time employees (FTE) on their vendor management staff.

46%

report spending more than $5,000 on vendor risk management.

There are indications that the board and senior management are paying closer attention to third party risk management, evidenced by more spending dedicated to vendor management.

50%

say vendor management reports to the executive team and risk committee.

There's been a continued trend in organizing third party risk management as a function independent of the lines of business. Fortunately, only 2% of companies still embed vendor management in a line of business.

73%

of respondents believe third party risk management is getting more scrutiny by the regulators.

Only 2% of respondents believe that regulatory scrutiny of third parties is lessening.

venminder

Survey **Results**

COMMITMENT TO VENDOR MANAGEMENT

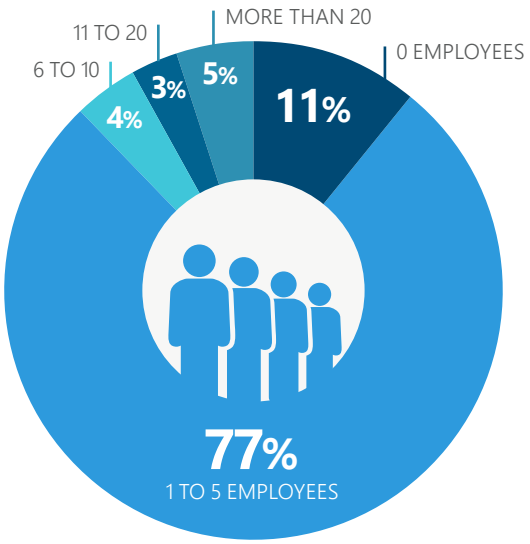
Internal Resources Committed to Vendor Management

Slight improvements but still room for more investment

More than three-quarters (77%) of respondents have five or fewer FTEs committed to working in vendor management. This is an improvement from 90% last year, perhaps due to adding new company types across the surveyed financial services and financial technology industries.

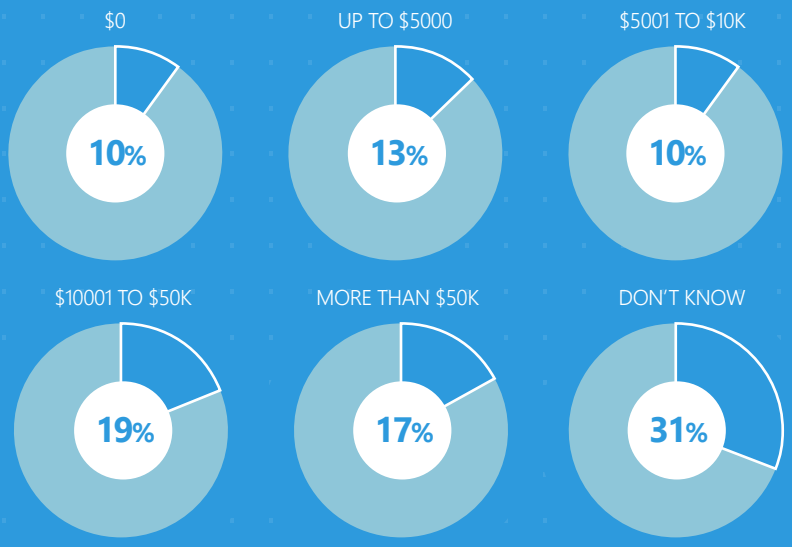
Within banks, 87%, including several banks over $10 billion in assets, have fewer than five FTEs. Within credit unions, 96% have fewer than five FTEs, which isn't surprising since credit unions are typically smaller than banks. The fintech and non-bank lenders, possibly due to pressure from their bank and credit union clients, are devoting more resources to vendor management. Several fintech firms note having 20 or more FTEs involved in vendor management.

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

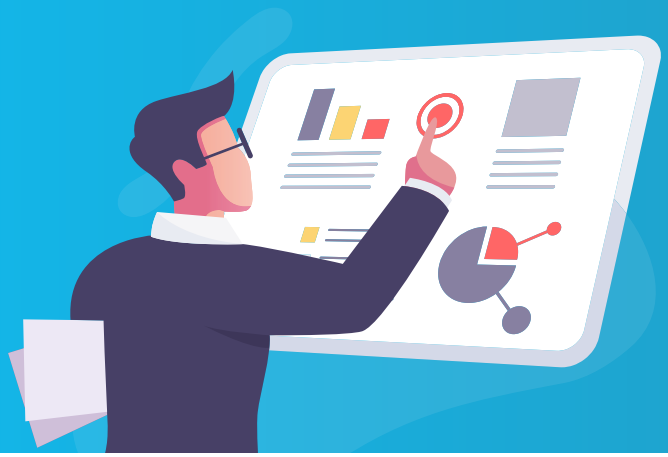


Given the challenges of third party risk management, particularly at smaller companies where vendor management may be an afterthought for the already overwhelmed compliance manager, it's important that the function is appropriately staffed with people sufficiently trained to do the job.

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



Interested in a deeper dive?
Download our supplemental report for company type and size breakdown.
Click here.



76%

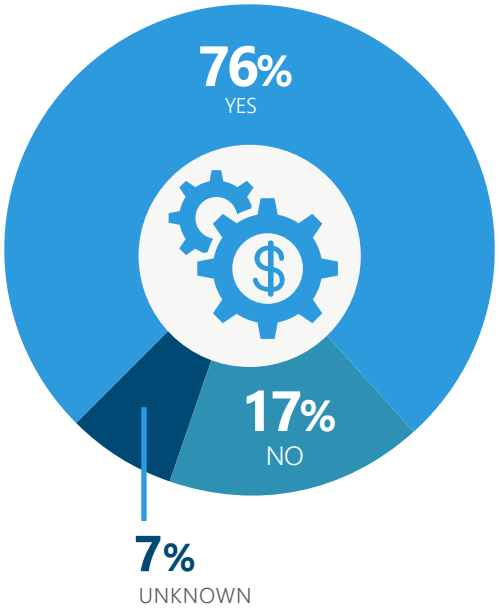
of respondents believe there is a **return on investment (ROI)** from efficient vendor risk management.

One-third (33%) of respondents report spending less than $10,000 on vendor management, not including direct personnel expenses. Last year, 53% of respondents spent less than $10,000 but the presence of insurance companies influenced this year's overall response since only 17% of insurance respondents report spending less than $10,000.

As expected, larger companies spend significantly more on vendor management than smaller companies. Hopefully this spending reflects a genuine concern by senior management and the board to invest in such an important function. 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 company'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 company spends on its physical appearance, isn't it worth spending at least that much on its compliance, operational and reputational risk?

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



A new question for this year's survey found that more than three-quarters (76%) of respondents believe that vendor management delivers ROI.

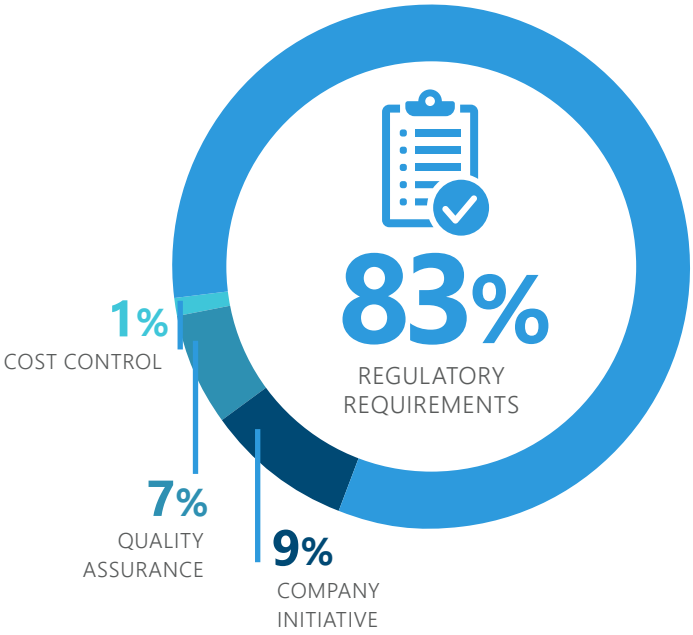
We suggest that those who don't see a link between vendor management and ROI explore how a well-managed program can drive real cost savings by preventing unwanted automatic contract renewals and by performing champion/challenger scenarios to find the most cost-effective vendors. It's very likely these companies will be surprised at how much they can save.

The fintech respondents overwhelmingly (96%) see an ROI benefit in vendor management, hopefully an indication that fintechs will continue to innovate with the right risk-related approach in mind. It's interesting that mid-sized credit unions saw the least ROI benefit—and in a few pages we'll see that they are also among those facing the biggest vendor management challenges.

Not surprisingly, the vast majority of respondents (83%) do vendor management to satisfy regulatory expectations. Encouragingly, fintech and non-bank lenders, and to a smaller extent wealth management and insurance, embrace vendor management to support company initiatives rather than cost control.

It's encouraging that cost control is almost never the primary driver of vendor risk management. If cost was the main driver, companies may be tempted to water down risk management and select the cheapest solution. Risk and regulatory expectations must always be the lighthouse on the rocky shoreline that vendor managers and compliance officers follow as their guiding beacon.

What is your primary reason for doing vendor risk management?



83%

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

Organizational Structure

Independence from lines of business continues

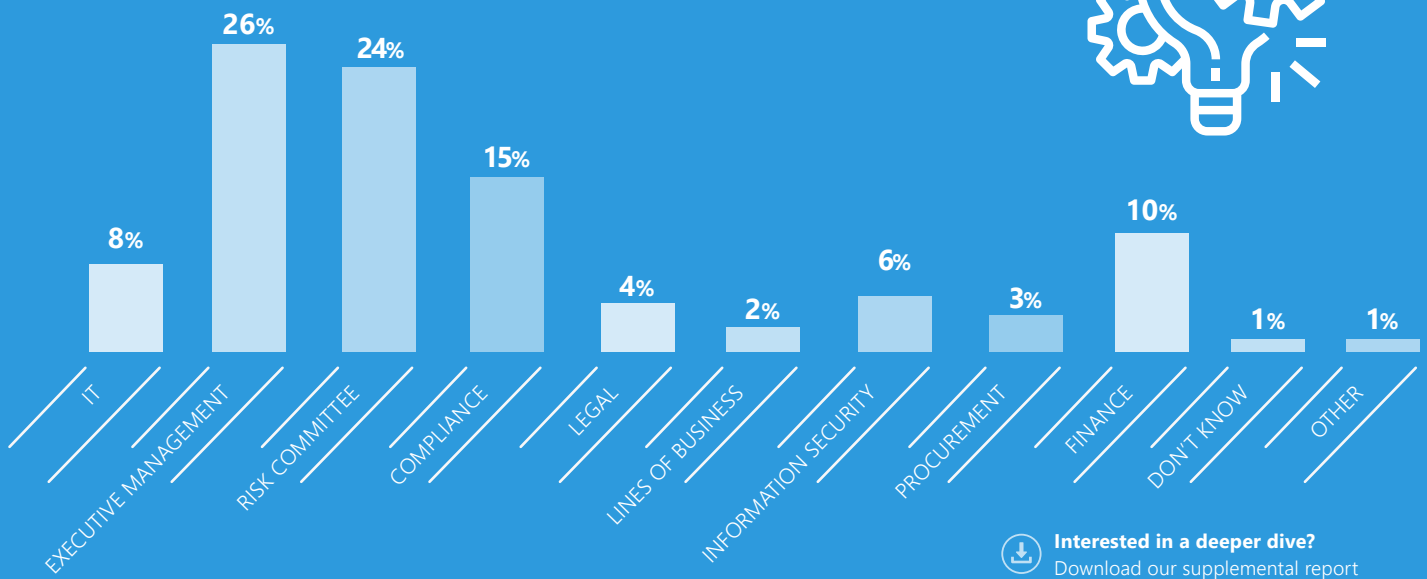
As organizations grow and mature, and as regulators issue guidance on active board involvement, third party risk management practices must evolve. The best practice and industry de facto standard is to have third party risk management independent from the lines of business and back office functions.

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. It's good news that only 2% of respondents report that third party risk management reports to a line of business while 50% of total respondents and 54% of banks say that executive management and the risk committee control vendor management activities.

Larger organizations, with typically more disciplined processes and more rigorous risk management practices, tend to have third party risk management report to executive management or the risk committee. However, giving the business units a voice in third party risk is important so the business cannot ignore risk management implications when outsourcing a key product or service.

Since IT can be swayed by favorite vendors, cost considerations or ease of implementation rather than risk, it's concerning that 6% of companies say that third party risk reports to IT.

Where does vendor management report to?



Interested in a deeper dive?
Download our supplemental report for company type and size breakdown.
Click here.

Sponsorship from the Top

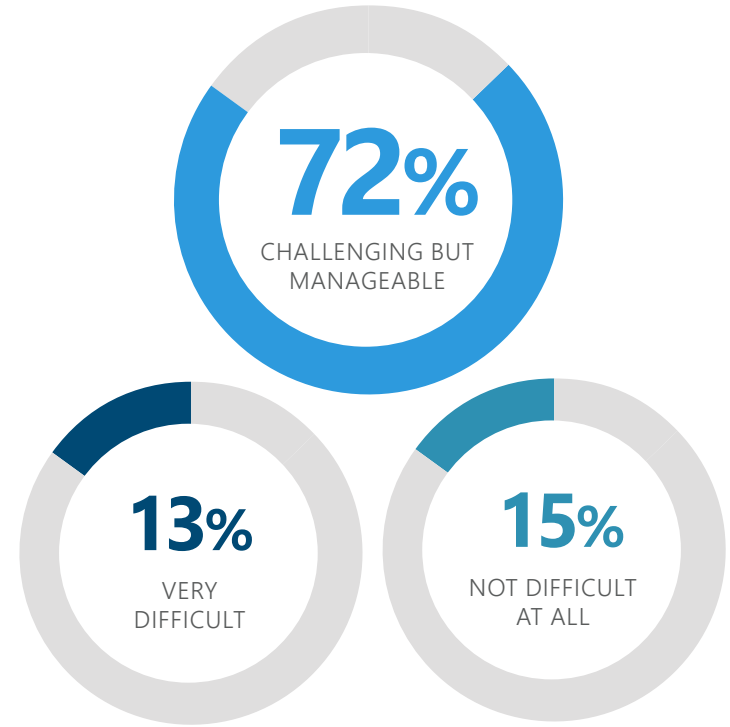
Setting the tone from the top is important

Interestingly, almost the same number of respondents find vendor management very difficult (13%) or not difficult (15%) at all. But those respondents were dwarfed by the 72% who say that vendor management is challenging but manageable, nearly identical to last year. The very smallest and very largest companies reported that vendor management is not challenging at all!

It's encouraging that companies are managing to adapt to regulatory expectations. Of course, with the exception of FHFA Bulletin 2018-8, there has been no significant new third party guidance issued this past year. The FFIEC guidance and the OCC bulletins are generally regarded as the strictest regulations so it's no surprise that banks and credit unions feel the most challenged. The good news is that these companies that manage risk to the most stringent guidance and best practices will always be well ahead of the game.

It's incredibly important that senior management takes vendor management seriously and is willing to stand behind the vendor manager 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.

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



72%

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 companies, vendor management is complex

As expected, the number of vendors managed varies by company size, with larger companies managing more vendors than smaller firms. Vendor management is industry-agnostic and all companies must approach this function commensurate with their size and complexity.

With so much pressure on margins in today's competitive landscape, one way to cut costs is to outsource functions. However, companies 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.

Use these statistics for insight into how your company stacks up against others in terms of scope of vendor management. We encourage clients to verify that descriptions of actively managed vendors are up-to-date, accurate and identify which 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.

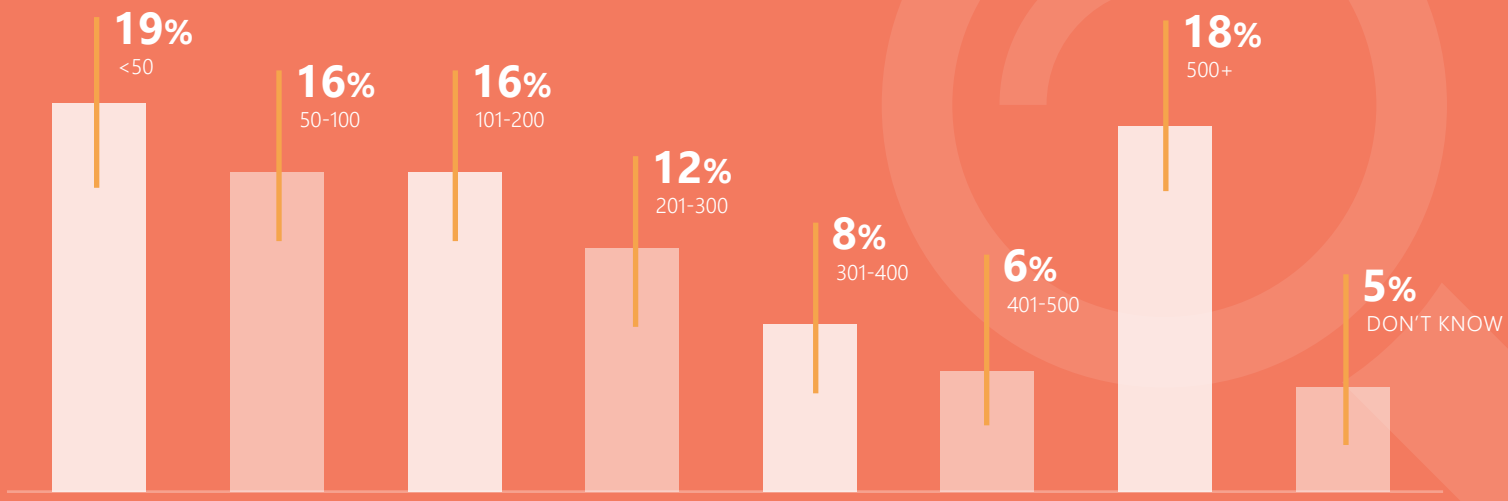
18%

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?



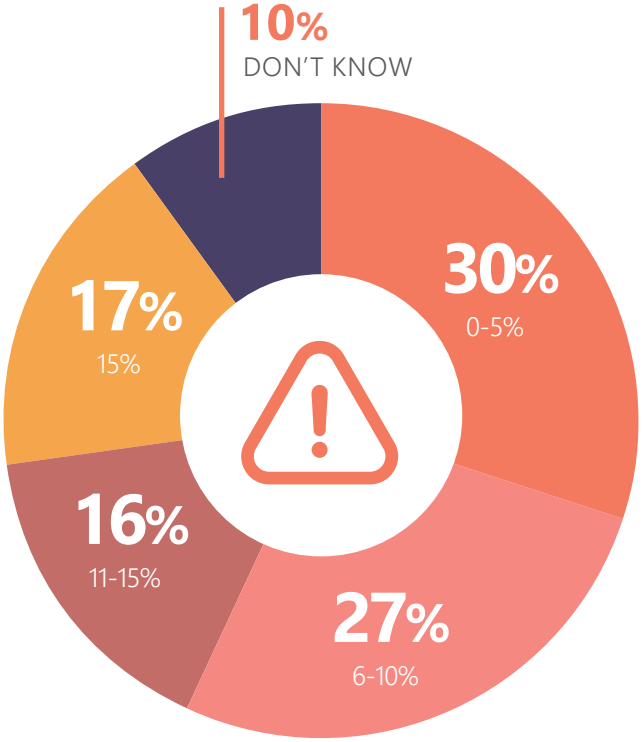
Interested in a deeper dive?
Download our supplemental report for company type and size breakdown.
Click here.

Companies typically classify about 10% of their vendors as critical. These results do not change much from year to year, indicating that firms 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 who report that more than 15% of vendors are critical, revisit how many core services are outsourced and how aggressively they need to be managed. Interestingly, wealth management and insurance have a higher percentage of critical third parties than other respondents, perhaps because they rely on so many external services to fulfill obligations to their customer base. If a sudden loss of the third party would cause a material disruption to your company or your customers, consider that vendor critical and plan accordingly.

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



51%

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

Technology Tools Used

Marching toward more automated solutions

Just over half (51%) of respondents indicated that they use a dedicated software platform to manage third party risk management. Not surprisingly, the larger and more sophisticated companies gravitate to this approach. Some firms (18%) – those likely more concerned with overall risk – use their Enterprise Risk Management (ERM) solution for vendor management. We believe this is a mistake since ERM solutions are not designed for vendor management and don't have the functionality to do vendor management well.

A surprising number of companies (21%) still rely on Excel. While Excel can be a great tool for other functions, having to open up hundreds of spreadsheets just to change a single field if a technical requirement in the regulatory guidance changes is time-consuming and error prone.

What is your primary tool for managing your vendors?

21% EXCEL

3% ACCESS DATABASE

51% A DEDICATED VENDOR MANAGEMENT SOFTWARE PLATFORM

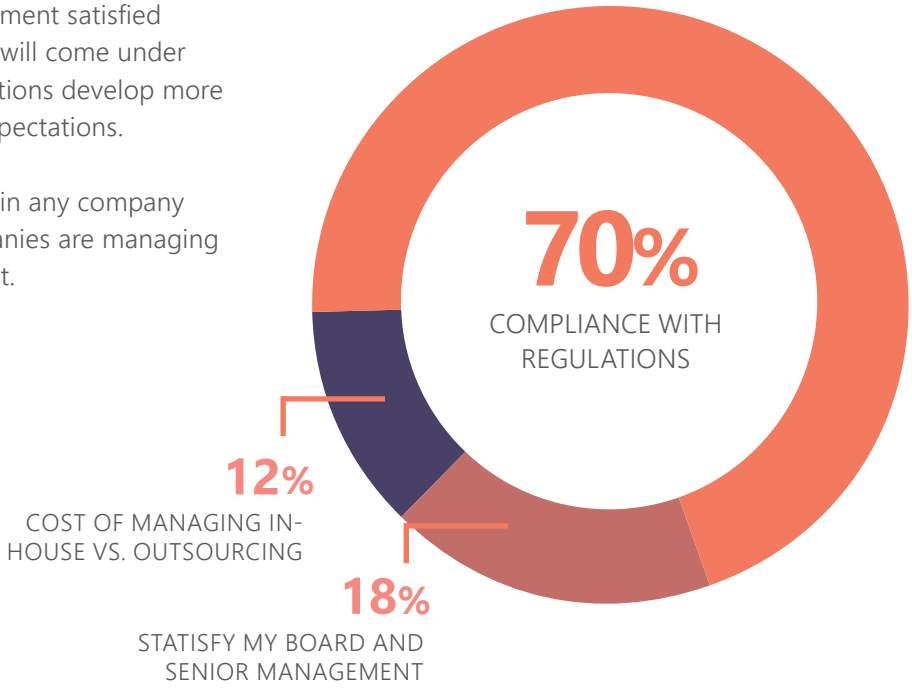
18% A VENDOR MANAGEMENT MODULE INSIDE OF AN ERM PLATFORM OR GRC

7% OTHER

Fortunately, regulatory compliance is the number one consideration for 70% of respondents. Those respondents less stringently managed for third party risk, such as fintechs, tend to cite keeping management satisfied as most important. However, fintechs will come under additional pressure as financial institutions develop more structure around their fourth party expectations.

Cost is not a prevailing consideration in any company type, an encouraging sign that companies are managing risks and expectations rather than cost.

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



70%

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?

Interested in a deeper dive?
Download our supplemental report for company type and size breakdown.
Click here.

Best Practices in Vendor Management

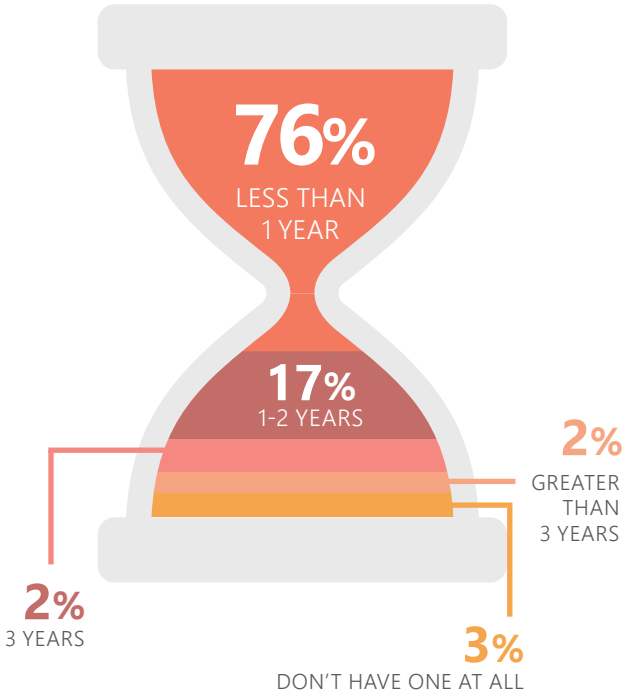
Several tried and true methods continue to stand the test of time

A majority (77%) of respondents, with the exception of wealth and asset management, require a pre-contract risk assessment, an improvement from last year's 67%. The pre-contract risk assessment is not only a best practice and general industry standard, but informs management of the risks they are 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.

The 2013 OCC guidance, Bulletin 2013-29, set the stage for the notion of not only doing a risk assessment at the onset of a relationship but taking an active lifecycle approach to keeping an eye on risk throughout the life of the relationship.

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



Keeping your vendor management policy documents up-to-date and consistent with regulatory guidance and best practices is incredibly vital to having a successful practice. This year, 76% say they update the policy at least yearly, a slight improvement from last year's 74%. 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.

Of concern is the 3% of companies that do not have a policy at all. Vendor management requires structure and discipline and regulated companies need to prove to regulators that they have read and understand the guidance. A written policy accomplishes that goal.

Operating Models

More than half of respondents have a centralized model

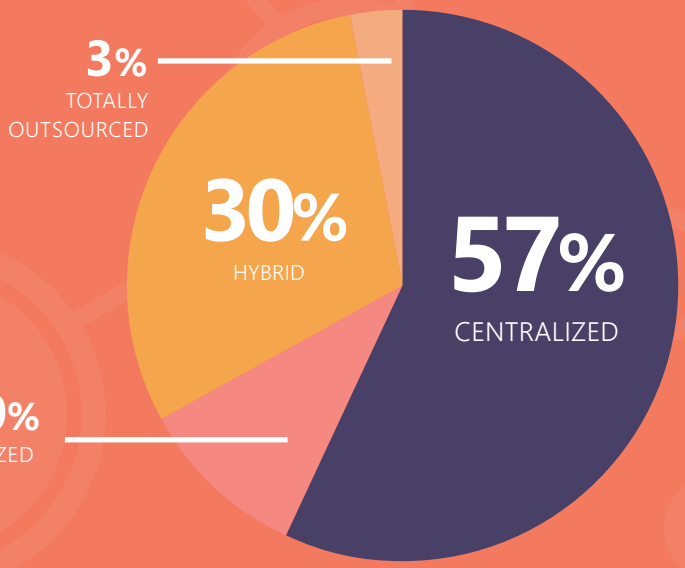
This year's and last year's findings on operating models are nearly identical. Larger and more complex firms with vastly different business unit functions often need to rely on a hybrid approach; it can be nearly impossible to set standards that will work for the entire organization. This is especially true if the company is deliberately keeping third party risk group staffing low.

Bank holding companies that grew up through mergers and acquisitions and have more diversified business models tend to rely on hybrid or decentralized solutions while many of the smaller institutions rely on a centralized or perhaps hybrid approach.

Even those companies with a centralized solution still need to keep front line management informed. Front line management are often the best eyes and ears about potential changes in third party risk. If you deploy a hybrid solution, dictate clear standards just as you would in a decentralized solution and be 100% certain that each party's role and responsibilities are clear to avoid gaps or wasteful overlaps.

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

Interested in a deeper dive?
Download our supplemental report for company type and size breakdown.
Click here.



STATE OF THIRD PARTY RISK MANAGEMENT

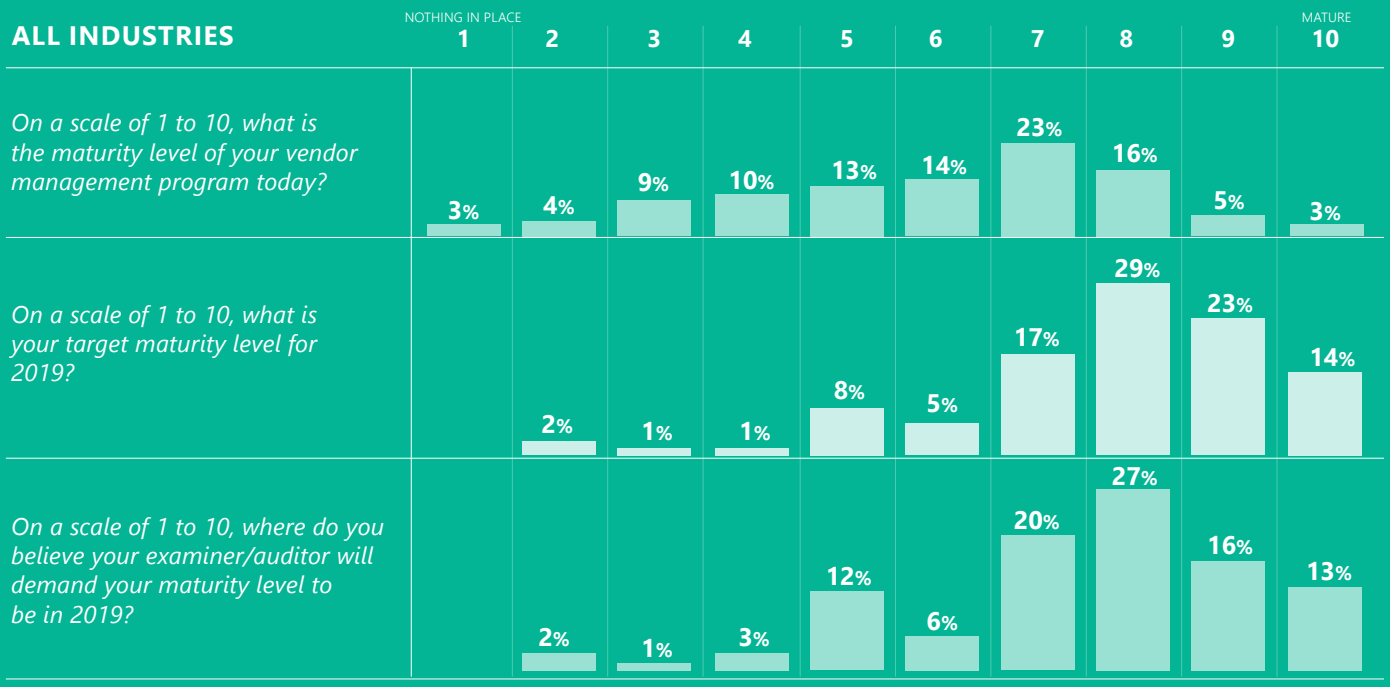
Maturity of Vendor Management Program

The roll toward 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.

There are no areas in which respondents say, "We've overmatured and perhaps can dial it back a notch." Respondents show that they are concerned about heightened expectations and regulatory requirements yet express an eagerness to evolve toward greater maturity in their processes.

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 2019 and where they believe the examiners/auditors will demand the maturity level to be at in 2019.

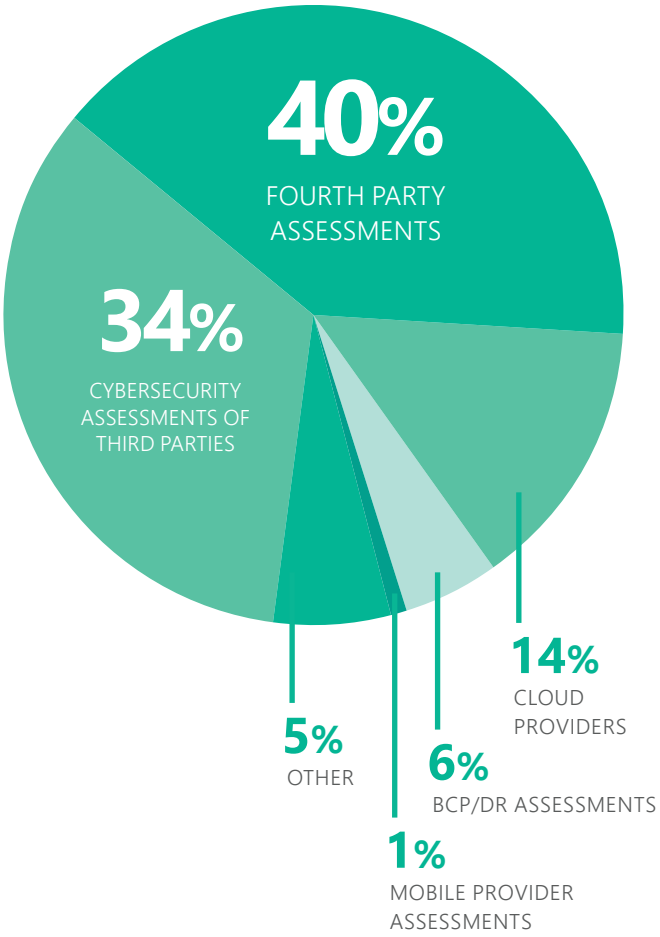


Wealth and asset management report the least mature programs, perhaps because their programs simply haven't received as much regulatory scrutiny. However, wealth and asset management also has the widest gap between their current and target maturity levels, indicating they understand they have a lot to do to develop a mature vendor management program.

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.

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 NCUA's current guidance dates all the way back to 2007. Think about how much technology, such as mobile banking and remote deposit capture, has changed in the past 12 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.

What do you see as your next biggest hurdle?



FDIC and OCC regulated institutions 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.

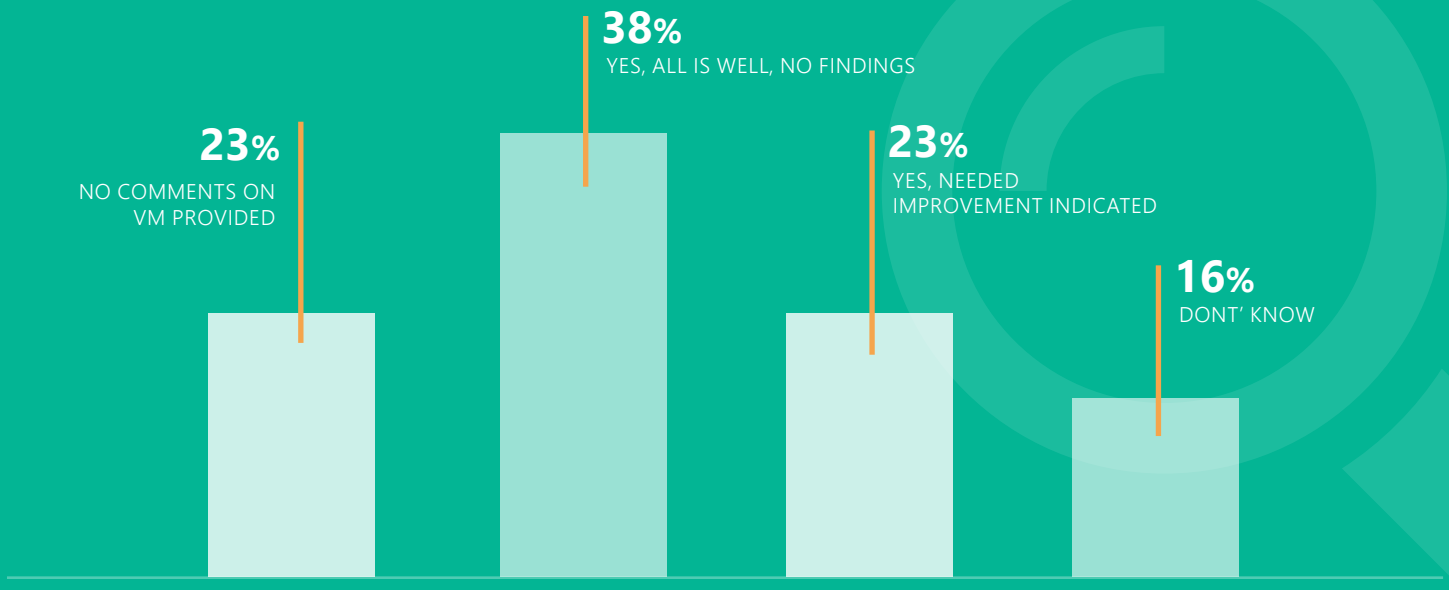
Finally, fintechs also recognize that they need to step it up a notch to be in compliance, definitely to meet financial institutions' expectations and certainly if they plan to apply for the new OCC Fintech charter, which essentially holds fintech companies to the same rigorous standards as national banks. 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.

Three-quarters of respondents are focused on the hot button topics of cybersecurity (34%) and fourth party risk management (40%). We were surprised that mobile provider assessments didn't garner more concern but that's likely because companies are so focused on other issues. Cybersecurity absolutely needs to be a front burner issue for the industry; in an era when it's not a matter of "if" but "when" an incident will occur, companies need to be poised to react and the best way to do that is to prepare well in advance.

With pressure mounting to create a national standard around data protection in the United States akin to the European Union's General Data Protection Regulation (GDPR), information security is going to continue to be a focus in 2019.

While there has been very little mention in formal guidance regarding fourth parties, examiners are laser-focused on companies that have even tangential access to customer data and what the third party is doing to protect it. In fact, at two recent industry conferences, there were very specific questions about the role of fourth parties. While we await guidance, the unwritten expectation is that fourth parties must be a risk consideration. In theory, it should be a bit easier to discern who these fourth parties are since they will be disclosed on the new SSAE 18 reports.

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 company type and size breakdown.
Click here.

Exam Results

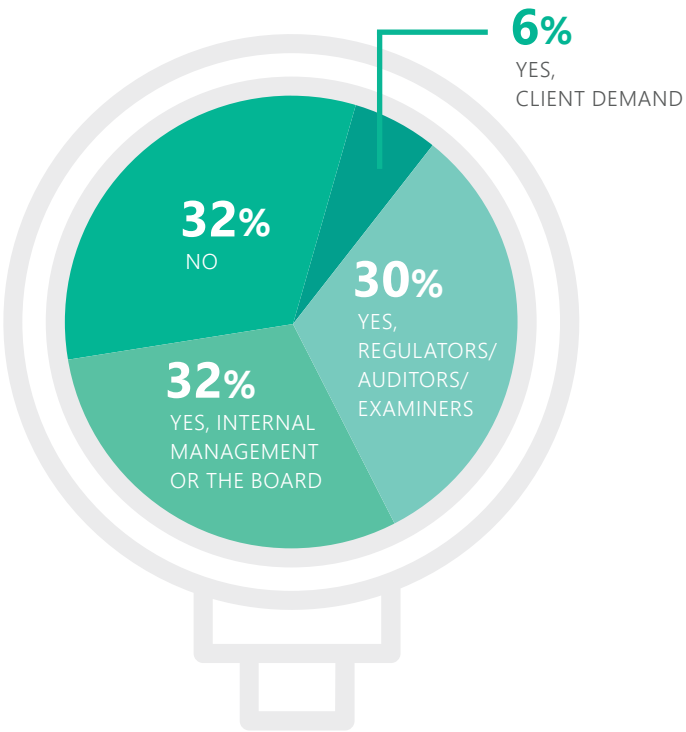
Signs of increased regulatory focus on vendor management

Nearly a quarter (23%) of respondents say that their most recent exam indicated that they need to make improvements.

Don't let your guard down even if your exam indicated no comments or no specific findings related to vendor management. No news is not always good news; it could be that it was not an area of exam focus. Vendor management winds its way through numerous regulations and could come up in any examination, particularly if you outsource key functions.

Two-thirds (62%) of respondents feel pressure to improve third party risk management, with much of that pressure coming from the board and regulators. It's interesting that mid-sized companies feel the regulatory pressure the most, consistent with the finding that mid-sized companies rate the perceived difficulty of doing third party risk management higher than other companies.

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

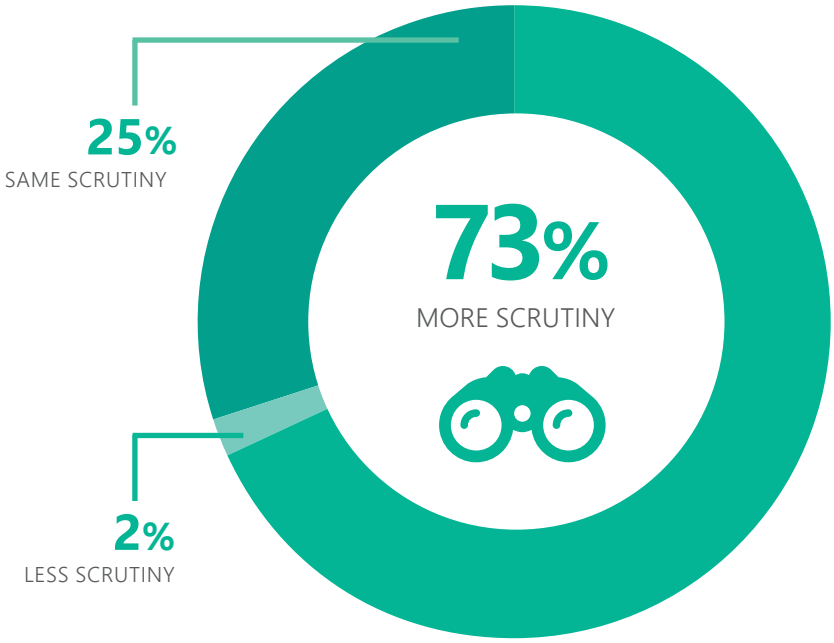


The regulatory bar keeps getting raised, with new SSAE 18 standards, FinCEN guidance on enhanced customer due diligence and huge fines around UDAAP (Unfair, Deceptive or Abusive Acts or Practices) and AML (Anti-Money Laundering) issues. The need to discern with whom you're doing business and properly oversee their activities is at an all-time high. We always suggest looking closely at enforcement actions for any issues that may be present in your own company; it's better to learn lessons from others' actions.

Boards feel the pressure as well, thanks to OCC Bulletins 2013-29 and 2017-7 which clearly spell out the need for active board involvement, and that pressure is being pushed throughout the organization.

This survey result should come as a shock to no one: only 2% of respondents believe that third party risk is getting less attention from the regulators while the overwhelming majority (73%) feel it's getting more attention and 25% believe it has stayed the same. Not a single bank or credit union says that third party risk is getting less attention.

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



As further proof of regulatory scrutiny, a former senior Treasury official rattled off his top concerns at the PRMIA (Professional Risk Management Industry Association) conference in Washington, DC, in November 2018 and the top two concerns were cybersecurity and operational risk, both of which have third party risk management written all over them. If that's not a good indication of how much focus our industry is getting, we don't know what is.

73%

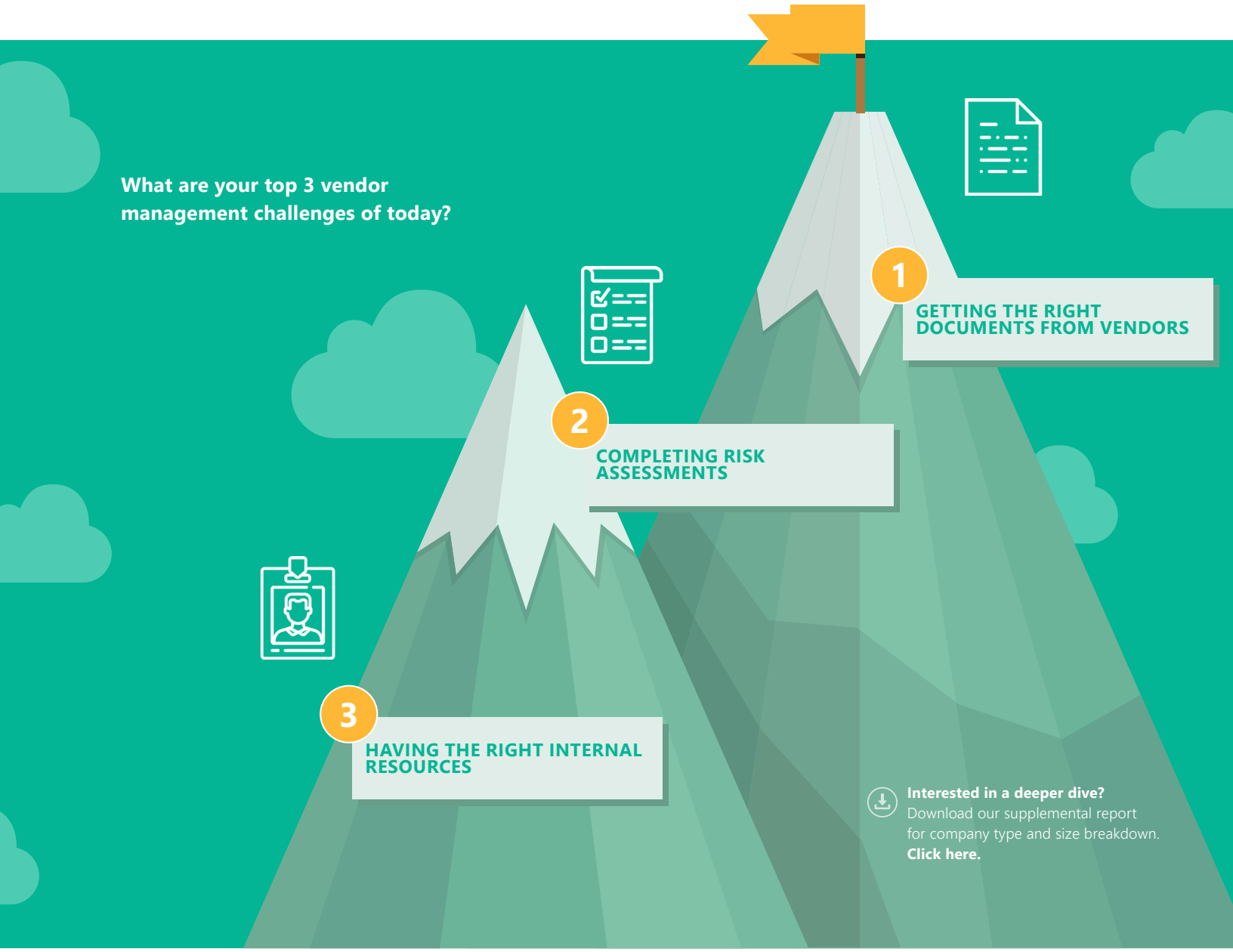
of respondents believe third party risk management **is getting more scrutiny by the regulators**.

Vendor Management Challenges

Getting the right documents is still an issue

For the second year, gathering documents from vendors continues to be one of the biggest vendor management challenges. Those companies not as strictly regulated by point-by-point prescriptive guidance, such as fintechs and non-bank lenders, are more concerned about risk assessments and having the right internal resources.

Interestingly, bankers at the FDIC community banking conference expressed concern, even frustration, at being held to task for not getting the right documents. Bankers say it's a real dilemma when large processors or key service providers aren't forthcoming in providing documents yet these smaller banks can't afford to simply walk away from these vendors.



RECOMMENDATIONS & BEST PRACTICES

Insights from working with hundreds of clients

Regulatory reform was passed in 2018 but no one felt any relief from lessened expectations around third party risk management. The only real change was extending the exam cycle from 12 months to 18 months for institutions with less than $3 billion in assets.

If creating or refreshing your vendor management program has not been high on your priority list, move it up the list. Vendor risk management must be an annual and "as needed" exercise that includes getting approval from the board and senior management. For those companies 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 regulatory requirement and was reiterated in the OCC Bulletins 2017-7 and 2017-21, so make creating meaningful board level reporting and capturing those results in minutes of senior management a priority.

Finally, with the intense focus on cybersecurity and increased expectations around the role that fourth parties play — even though new SSAE 18 standards require disclosure of significant subservice providers — the working relationship between your company's vendor management program and information security requires ongoing development.

The state of vendor risk management is clear: regulatory expectations are increasing and companies across industries are scrambling to keep up with the changing landscape. Focusing on the tried and true basics of vendor management will only get you half way; you'll need adequate resources and sophisticated tools to properly manage the risks outsourced service providers pose to your company.

venminder

Here are 10 best practices to get you started in reaching desired maturity levels in an efficient and executable manner.

Make sure your company:

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. Ensures 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 updates all documents and practices
9. Adequately and effectively performs ongoing monitoring and follows up on deficiencies
10. Keeps a close watch on consumer complaints as they are often the fodder for enforcement actions

ABOUT VENMINDER

Venminder is the market leader in third party risk management solutions. Through the firm's software and suite of outsourced services, Venminder has pioneered a new age of vendor management by dramatically reducing the workload essential to meeting today's demanding regulatory requirements.

Venminder's software organizes all things vendor-related and guides users through critical processes such as contract management, risk assessments, due diligence requirements, questionnaires and more. The firm also offers a popular suite of outsourced due diligence services which includes collecting documents and then assessing them for risk in cybersecurity, information security, business continuity/disaster recovery and financial health.

Venminder is currently used by over 600 financial services and financial technology firms. As all of their solutions are scalable, Venminder clients range in size from small to very large organizations.

STAY UP-TO-DATE WITH VENMINDER

- Webinars
- Industry Interviews
- Videos and Podcasts
- Blog

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

NEED ASSISTANCE? LEARN ABOUT VENMINDER'S

- Software
- Outsourced 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 company type and size.

venminder

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