



Mind the Gap – Where Third-Party Risk Management Programs Fall Short

Results of the 2020 TPRM Benchmarking Survey

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily email newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com



Aravo delivers market-leading solutions for understanding, managing, and mitigating the risks posed by third-party vendors and their engagements. Using Aravo, customers maintain a single, auditable inventory of all third-party relationships and can automate risk assessments, scoring, due diligence, continuous monitoring, issue management, and corrective actions. Built on technology designed for usability, agility, and scale, Aravo supports complex custom-configured solutions used by many of the world's largest global brands as well as pre-configured applications that allow clients to stand up a best-practice program quickly and confidently. www.aravo.com

Inside this e-Book

Introduction	4
Use Data, DOJ Mandate to Make Business Case for Beefing Up TPRM	5
Expert Sounds Alarm On Survey Results: Lack of Resources ‘Striking’	7
Highlights	9
Resourcing	10
Incidents	13
Lifecycle Management	15
The Board and Third-Party Risk	17
Program Maturity	18
Results	19
Part 1: Maturity and Age	20
Part 2: Third-Party Incidents	25
Part 3: The Board and Third-Party Risk	28
Part 4: Third-party Risk Organizational Structure, Resource, and Budget	32
Part 5: Third-Party Universe and Program	38
Part 6: Technology	45
Part 7: Challenges and Opportunities	49
The Final Word	61
Methodology & Demographics	63

Introduction

Third-party risk management (TPRM) is an evolving, and often complex, discipline. Regulatory change, the scope of existing and emerging risks, and deeper requirements, particularly those around 4th and Nth parties, ensure the environment is dynamic and ever-changing. And now, as the world grapples with a pandemic and its consequences, even more is at stake in how we view and manage risk, so as to 'bounce forward' and build additional resilience in our businesses and our supply chains.

This is the third year of the "Taking the Pulse of Third-Party Risk Management" survey. The survey is designed to provide a broad and deep analysis of how third-party risk management is evolving and to provide important data points to help firms benchmark their programs and identify emerging best practices.

This year's survey took place between February and early March 2020, before the full force of Covid-19, so it's important to note that this was not a focus of the survey at the time, but is likely to have repercussion on programs.

Once again, we would like to extend our deepest thanks to all of those who participated in the survey. Their willingness to share their experience will contribute to the development of the discipline. We hope the findings of the survey will help organizations further refine their roadmap to maturity and support the many decisions teams will have to take along that journey.

Use Data, DOJ Mandate to Make Business Case for Beefing Up TPRM

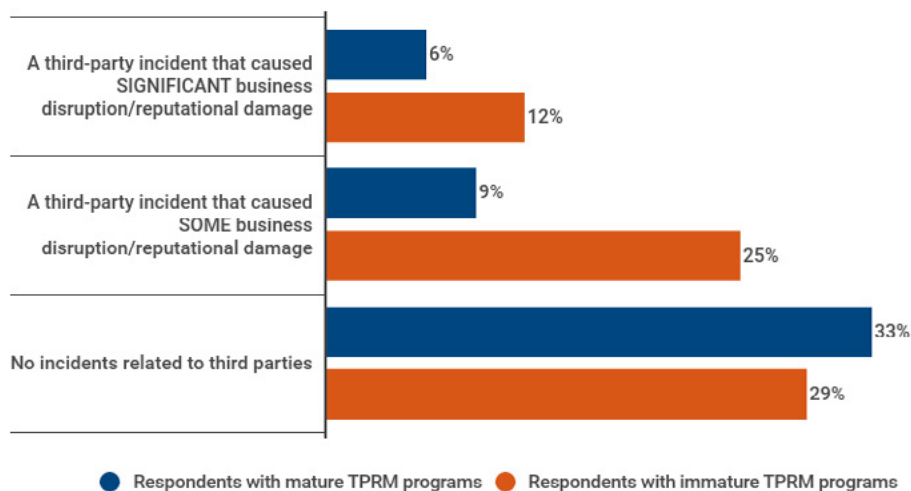
By Dave Lefort, Compliance Week

Third parties are mentioned [33 times](#) in the Department of Justice’s updated “[Evaluation of Corporate Compliance Programs](#)” released in June, meaning that if you weren’t paying close attention to what your partners are up to—and according to a recent survey, many of you weren’t—you’ve officially been put on notice.

Broadly, the updated DOJ guidance says compliance programs will be judged by prosecutors on whether they are “adequately resourced and empowered.” Reading between the lines, that means compliance programs need to be funded and staffed at a level appropriate for their risk profiles. When it comes to third-party risk, many companies aren’t meeting that standard, according to a new poll by [Aravo](#) and Compliance Week.

What’s the best way to ensure your program is adequately resourced? Make a business case, of course. If your program doesn’t meet the DOJ guidelines, your business is at risk for heavy fines and reputational damage. The best protection against that is a robust, mature, risk-based third-party management strategy. A better program is a sound investment, and the data bears that out:

In the last 12 months my company has had ...



- » Overall, 32 percent of 313 survey respondents indicated their TPRM programs were “optimized” and “mature.” Among those respondents, just 6 percent said they had a third-party incident within the past year that caused “significant” business disruption or reputational damage and just 9 percent had an incident that caused “some” damage.
- » Among those who had immature or inadequately resourced programs, the number that had “significant” third-party incidents doubled to 12 percent. An additional 25 percent (almost 3 times the “mature” cohort) said they had a third-party incident that had “some” damage.
- » Among respondents working for companies with more than \$1 billion in annual revenue and who said they had more than 10 people on their TPRM teams, 32 percent said they had no incidents related to their third parties over the past year and just 5 percent indicated they had an incident that caused “significant” disruption or damage. Among companies with the same annual revenue but fewer than 10 people working on TPRM, however, more than 3 times as many (16 percent) said they had a major incident and an additional 22 percent reported an incident that caused “some” financial or reputational damage.
- » To make matters worse, of that under-resourced group (more than \$1B in revenue, fewer than 10 people working on TPRM), it didn’t appear that an influx of resources was on its way: Just 10 percent of those respondents expected their TPRM budgets to increase significantly over the next year (and this survey was conducted before COVID-19 turned the world on its side).

Specific to third parties, the updated DOJ guidance directs prosecutors to consider **“whether the company knows ... the risks posed by third-party partners.”** Another TPRM-related question added to the new guidance related to ongoing monitoring: **“Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?”**

Again, let’s turn to the survey data for some troubling answers:

- » Among respondents working for companies with more than \$1B in revenue and fewer than 10 staffers dedicated to managing third parties, 26 percent work with at least 10,000 third parties and more than half said they worked with third parties in high-risk areas of the world. A group so small can’t possibly keep up with the government’s mandate to monitor your partners on an ongoing basis ... and those working with parties in high-risk areas of the world are asking for trouble.
- » Exactly 1 in 4 survey respondents answered “I don’t know” when asked how many of their third parties they’d classify as “high risk.” If you’re in charge of managing third-party risks for your company and you don’t know how many of your partners are of the “high risk” variety, you’d be wise to prioritize fixing that.
- » Just 13 percent of all survey respondents said they monitor all of their third parties on an ongoing basis. An additional 18 percent said they have ongoing monitoring set up for more than half of their third parties. What about the rest?

The data is clear: A mature, well-resourced program is not only more likely to meet the DOJ’s new guidelines for due diligence and ongoing monitoring of third parties, it’s also much more likely to help pay for itself as a result in a reduction of reputational and financial damage caused by third parties.

Expert Sounds Alarm On Survey Results: Lack of Resources 'Striking'



By Jaclyn Jaeger, Compliance Week

Thirty-three percent of respondents to a recent benchmarking survey conducted by Aravo and Compliance Week said their third-party risk management (TPRM) programs are inadequately resourced and 27 percent said they didn't have a team dedicated to TPRM, a trend one expert called "striking" and a recipe for trouble.

Third-party risk is a common risk factor not only in corruption cases, but in financial fraud cases as well, said Ephraim "Fry" Wernick, a partner at Vinson & Elkins and a former federal prosecutor and assistant chief of the Justice Department's Criminal Fraud Section.

"From experience investigating these cases for the Department of Justice, 99 times out of 100, when you come across a problem, it's because you have a third-party issue," Wernick said. "The need to beef up the resources is substantial."

Thirty-two percent of respondents who reported having no dedicated team, for example, said they manage between 5,000 and 49,000 third parties, while another 23 percent said they manage between 500 and 4,999 third parties. Four percent of this group said they manage more than 50,000 third parties.

The survey's findings are a clear indication that many companies' compliance programs aren't in line with the Criminal Division's revised "[Evaluation of Corporate Compliance Programs](#)," last updated in June. Under the revised guidance, new language was added directing prosecutors to ask companies whether the compliance program, which includes TPRM, is "**adequately resourced and empowered to function.**"

The previous version of the guidance more subjectively directed prosecutors to consider if the compliance program has been "implemented effectively." In practice, the revised guidance asks for hard metrics: "What is the overall percentage of compliance personnel in the compliance function? What are the dollars spent on compliance compared to other functions?" Wernick asked.

Ongoing monitoring

The survey's findings further revealed that most companies aren't addressing risk across the full lifecycle of their third-party relationships, as indicated by the 83 percent of respondents who are not conducting ongoing monitoring or due diligence on all their third parties.

As companies develop and maintain more and more third-party relationships over the years, ongoing monitoring will only become more difficult. When it becomes unfeasible to continuously monitor thousands or even tens of thousands of those relationships, many companies decide, instead, to periodically assess just a handful of their third parties at a time.

“You need to prioritize, based on risk,” Wernick said. Doing so ensures the compliance function allocates its limited resources wisely when assessing, monitoring, and mitigating third-party risk. How much risk a third party presents depends on several factors, including:

- » The geographical region of the third party;
- » The nature and extent of its interaction with foreign government officials, including state-owned entities or government agencies;
- » The nature of the third party’s operations (i.e., commercial agents, distributors, resellers);
- » The revenue stream that the third party generates for the company; and
- » Whether it has, or how long it has had, a trusting relationship with the company.

Wernick also urged companies to apply lessons learned internally as problems arise and not keep information in a vacuum. Frequently, the same gaps in oversight or omissions that led to one problem in one area, typically, are happening in other parts of the company, or are happening elsewhere in the industry or in other regions as it pertains to the same third party. “We’ve seen this happen time and time again in the third-party context,” he said.

This “lessons learned” concept is explicitly addressed in the Criminal Division’s revised guidance, as well.

Specifically, it directs prosecutors to consider the following question: **“Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company’s own prior issues or from those of other companies operating in the same industry and/or geographical region?”**

Senior manager leadership

As it relates to third-party oversight at the board and senior management level, the “Evaluation of Corporate Compliance Programs” guidance directs prosecutors to consider, **“What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?”**

Yet, the survey’s findings indicate that many boards still fail to grasp the extent of the risks that third parties pose to their organizations, as cited by the 40 percent of respondents who said their board doesn’t have a good handle on third-party risk. “Senior management needs to understand the risk profile of third parties,” Wernick said. “They need to be getting that feedback from people on the ground who are managing those third parties and then voicing that internally up the ladder.”

“This is an area of increasing exposure for companies,” Wernick added. Senior management needs to not only have a better handle on third-party risks, but also “make sure the resources are available, so that compliance professionals can do their job.”

“From experience investigating these cases for the Department of Justice, 99 times out of 100, when you come across a problem, it’s because you have a third-party issue.”



Highlights

This section of the report calls out some of the highlights of the survey results, with a focus on areas that third-party managers, senior management, and boards should pay heed to.

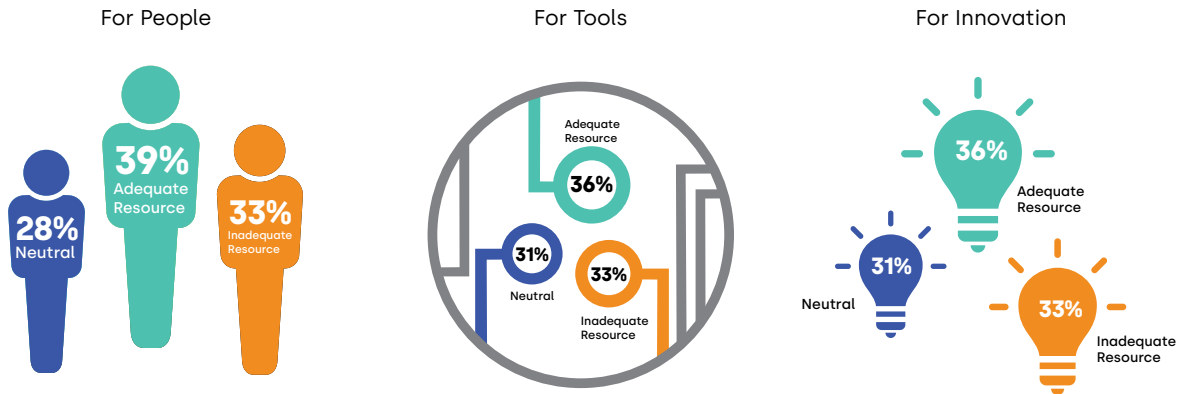
Resourcing

Resourcing is a key area of third-party risk management that requires attention.

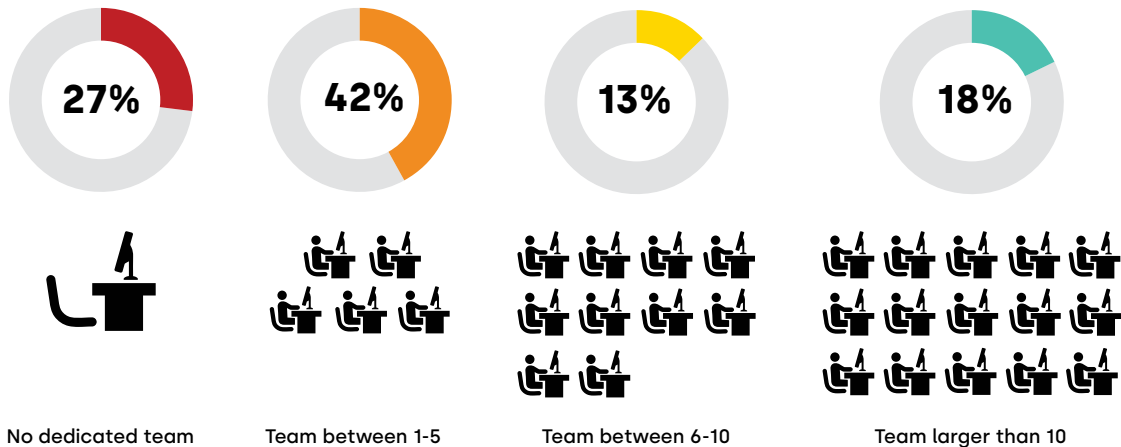
This is an area of weakness that boards and senior management should be concerned about as there is clear regulatory expectation that programs need to be adequately resourced and empowered.

Yet, insight from multiple sections of the survey illustrates that many third-party management programs are struggling to secure the resources and funding they require to be successful.

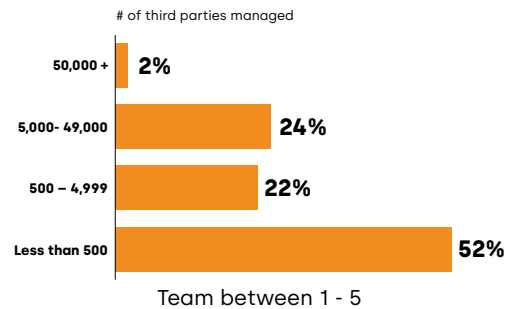
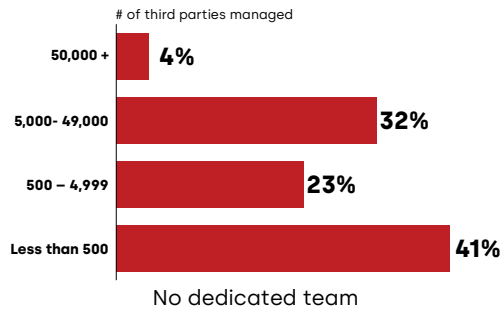
A third of respondents reported that they did not consider that their program had adequate funding for the people, tools, or innovation and continuous improvement necessary for the success of their programs.



A lack of resource is also evident in reported team sizes. Over a quarter of respondents (27%) indicated that they did not have a dedicated team to manage third-party risk at their organizations, and 42% reported that their teams were between 1-5 people in size.



Despite having no dedicated resource or small team sizes, organizations are having to manage a high volume of third parties. Over half of organizations with no dedicated team were still having to manage more than 500 third parties.

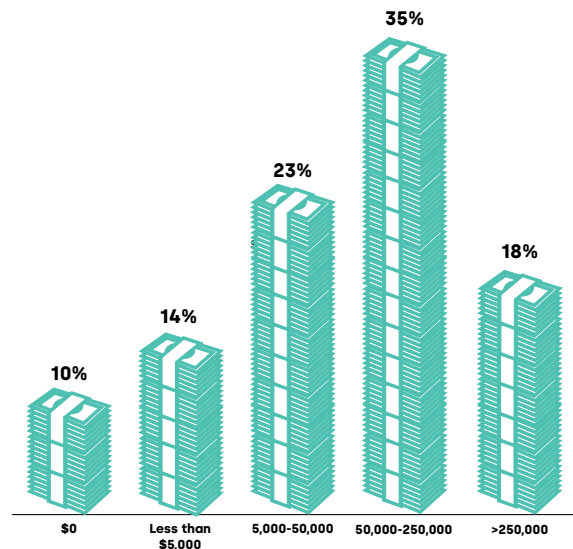


The lack of resource coverage here is alarming and something that organizations with small team sizes and large numbers of third parties should be looking to address.

In addition to a lack of coverage in headcount, budgets (non-headcount) were typically low as well, particularly considering the complexity and criticality of third-party risk management. Of those that did know their program budget, almost a quarter had a budget of less than \$5,000.

Further, most budgets were not anticipated to increase in the next 12 months, with 50% expecting their budgets to remain the same and 11% expecting them to decrease to varying degrees. This was prior to the full impact of COVID-19.

Resource was also a challenge that was called out in the qualitative section of the survey.



Many respondents mentioned the lack of resource to do the job properly, with typical responses including:

"Lack of staff to do a more thorough job"

"Lack of budget. Shrinking appetite for associated administrative burden considering no suppliers have been 'Denied' to this point"

"Having enough people to properly manage third-party risk"

"Being able to manage the amount of oversight and due diligence needed with limited number of resources"

"Obtaining necessary resources to bring program up to industry best practice"

"Getting budget to install and use a tool"

"Increased level of regulatory expectations without commensurate increase in resources/\$"

Others also specifically mentioned the challenge associated with getting senior management to understand the level of effort and budget required for third-party risk management:

"Convincing management of the need for more resources"

"Budget and support from C-suite"

"Human Capital and Management Buy-In"

"Getting Management to understand the work required to meet the Board's expectations"

"Getting buy-in from the line managers on the importance and the associated costs of due diligence"

Taking stock of resource, and ensuring there is enough to run an effective program, is an urgent area for organizations to address. The DOJ's Evaluation of Corporate Compliance Programs (Updated June 2020) has made it quite explicit that compliance programs (which include third-party risk management) are "adequately resourced and empowered." This means that programs need to be well funded and staffed. Clearly many are not.

Incidents

The volume of third-party related incidents that can and do cause business and reputational damage should also be a wake-up call for senior management and boards.

Additionally, the results suggest that program maturity appears to play an important role in protecting the organization against the damage associated with such events. This should provide added incentive for businesses to focus on maturing their programs.

Third-party related incidents that could damage the business and/or its reputation are common. More than half (59%) of respondents who had insight, said that they had experienced incidents associated with a third-party that caused, or had the potential to cause, business disruption/reputational damage in the prior 12 months.



Immature Programs (Ad-hoc - Fragmented)



% of respondents who reported significant business disruption or reputational damage



% of respondents who reported some business disruption or reputational damage

Mature Programs (Integrated - Agile)



% of respondents who reported significant business disruption or reputational damage



% of respondents who reported some business disruption or reputational damage

When the maturity of programs was factored into whether third-party incidents translated into damage for the organization, the results cast some important data points for those seeking to mature and improve their programs.

When we looked at the data across all incidents that caused damage, we saw a much larger proportion among those with immature programs.

Incidents were more likely to cause **significant** business disruption or reputational damage in immature (Ad-hoc – Fragmented) programs (71%) than in mature (Integrated to Agile) programs (18%).

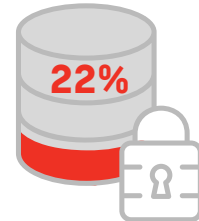
Incidents were also more likely to cause some business disruption or reputational damage in less mature programs (63%) than in mature programs (15%).

The most common forms of third-party incidents were related to performance, data breaches, regulatory compliance, and cybersecurity incidences such as hacking or malware.

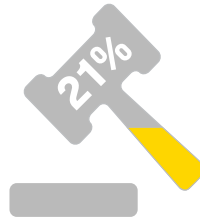
If you have had an incident, what was its nature?



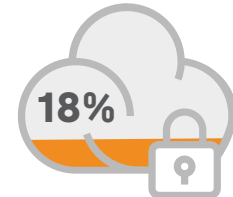
Performance / quality



Data Breach



Regulatory e.g. ABAC non-compliance, GDPR non-compliance



Cybersecurity incident

These are all important datapoints for third-party risk managers looking to build an internal business case for the value of a robust and mature program. Investments which advance the maturity of third-party risk management programs, help to protect the business from damage.

Considering the average cost of a data breach is \$3.92 million, and the average size of a FCPA enforcement action in 2019 was \$208 million, this should provide companies incentive to invest in maturing their programs.



CAUTION

Lifecycle Management

Despite regulatory expectation for third-party risk management programs to manage risk through the full lifecycle of the relationship, most programs do not.

In the June 2020 update to Evaluation of Corporate Compliance Programs guidance – there was a very specific update included, that guides prosecutors to assess:

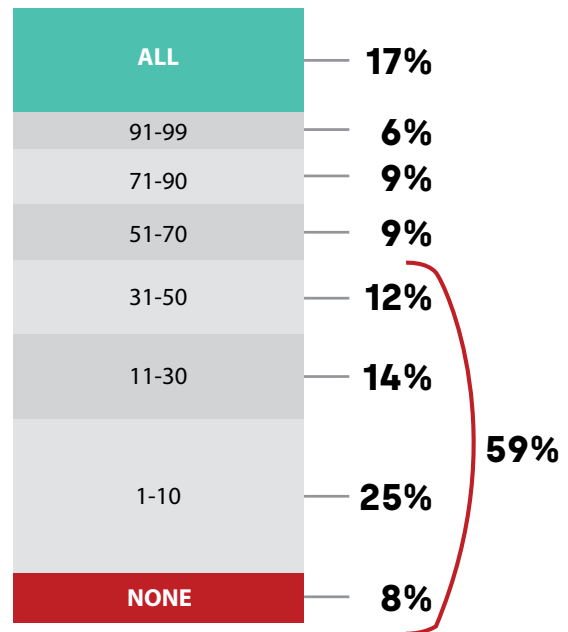
“Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?”

Again, the regulatory expectation is clear – regulators are looking for more than a ‘one and done’ approach. Rather, they are seeking evidence that the company is conducting ongoing risk monitoring and management throughout the term of the relationship. This requirement for lifecycle management is also a cornerstone of other regulatory guidance, including the OCC Bulletin 2013-29.

The survey revealed that most companies are not addressing risk across the full lifecycle of their third-party relationships.

The vast majority (83%) of respondents are not conducting ongoing monitoring or due diligence on all their third parties.

What percentage of your third parties have ongoing monitoring /due diligence conducted?



Our program addresses the full lifecycle of the third-party relationship



Fully
35%

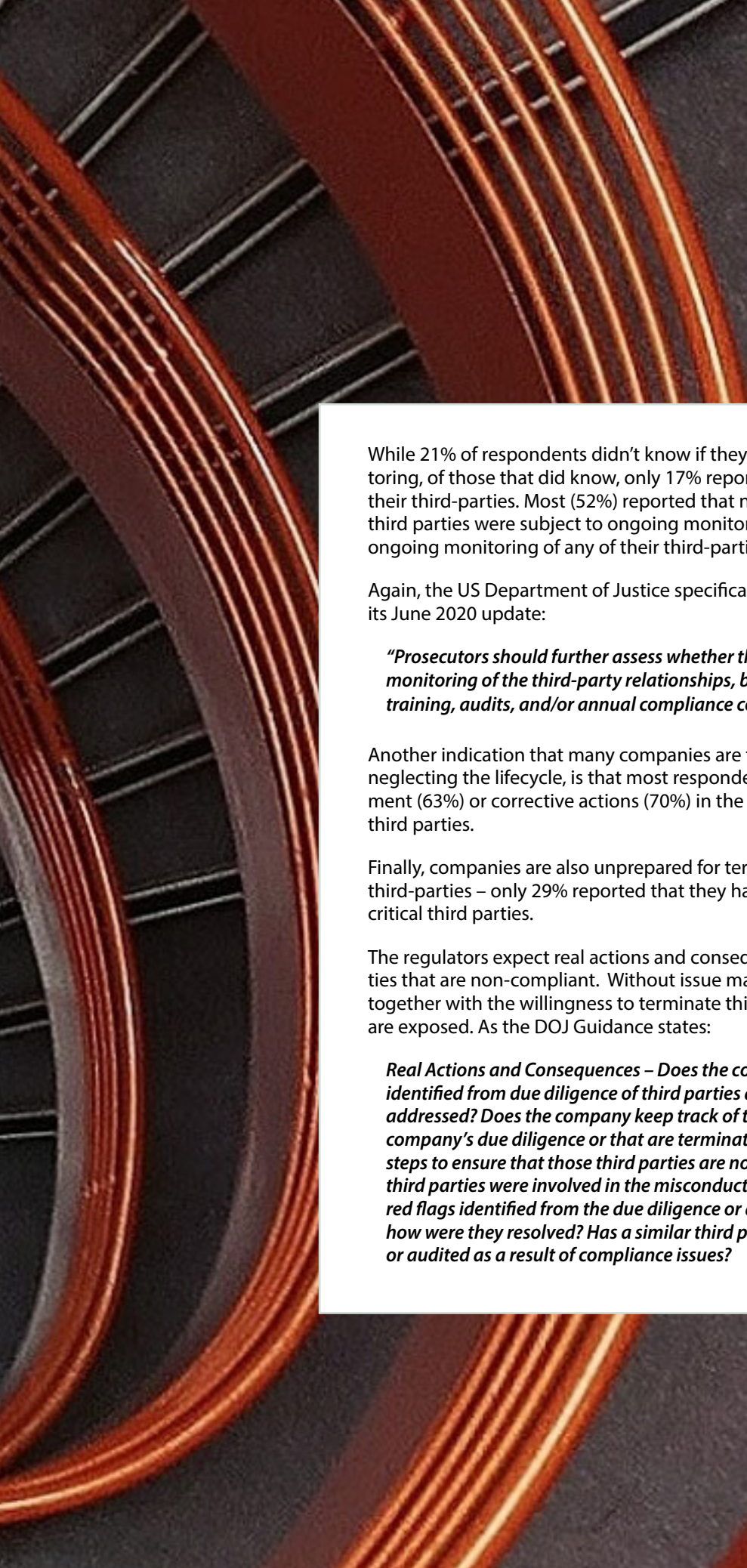


No
26%



Partially
39%

While 21% of respondents didn’t know if they were conducting ongoing monitoring, of those that did know, only 17% reported that were applying this to all their third-parties. Most (51%) reported that no more than half their universe of third parties were subject to ongoing monitoring/due diligence, and 8% had no ongoing monitoring of any of their third-parties at all.



While 21% of respondents didn't know if they were conducting ongoing monitoring, of those that did know, only 17% reported that were applying this to all their third-parties. Most (52%) reported that no more than half their universe of third parties were subject to ongoing monitoring/due diligence, and 8% had no ongoing monitoring of any of their third-parties at all.

Again, the US Department of Justice specifically calls out ongoing monitoring in its June 2020 update:

“Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.”

Another indication that many companies are focusing on onboarding, but neglecting the lifecycle, is that most respondees do not include issue management (63%) or corrective actions (70%) in the processes used to manage their third parties.

Finally, companies are also unprepared for terminating and off-boarding third-parties – only 29% reported that they have complete exit plans for their critical third parties.

The regulators expect real actions and consequences associated with third-parties that are non-compliant. Without issue management and corrective actions, together with the willingness to terminate third-party relationships, programs are exposed. As the DOJ Guidance states:

Real Actions and Consequences – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

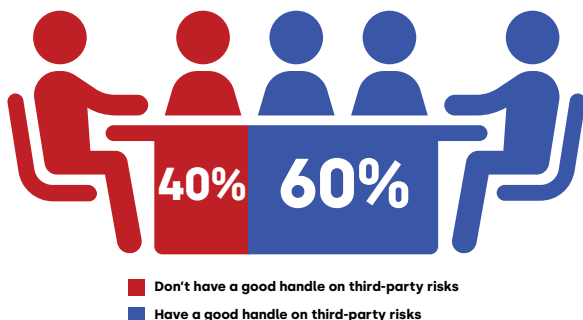
The Board and Third-Party Risk

Too many boards don't have a good handle on the third-party risks their organizations are exposed to.

One of the hurdles to having an effective third-party risk management program can be the board itself. The DOJ's Evaluation of Corporate Compliance Programs, states:

"The company's top leaders – the board of directors and executives – set the tone for the rest of the company."

Yet, while third-party relationships increasingly form a key part of business strategy, boards are failing to grasp the risks that third parties expose their organizations to. Some 40% of surveyed practitioners claimed that their board doesn't have a good handle on third-party risk.



This could be due in part to a lack of engagement in third-party governance by many boards – 34% percent of respondents indicated that third-party risk management was not a key priority for their board with only a low level of oversight.

Boards and senior management should understand that their engagement and oversight is an important component of program success and is expected by the regulators.

In respect to oversight, the DOJ guidance sets out:

Oversight – "What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?"

Board responsibility is also clear in OCC Bulletin 2020-10:

"However a bank structures its third-party risk management process, the board is responsible for overseeing the development of an effective third-party risk management process commensurate with the level of risk and complexity of the third-party relationships. Periodic board reporting is essential to ensure that board responsibilities are fulfilled."

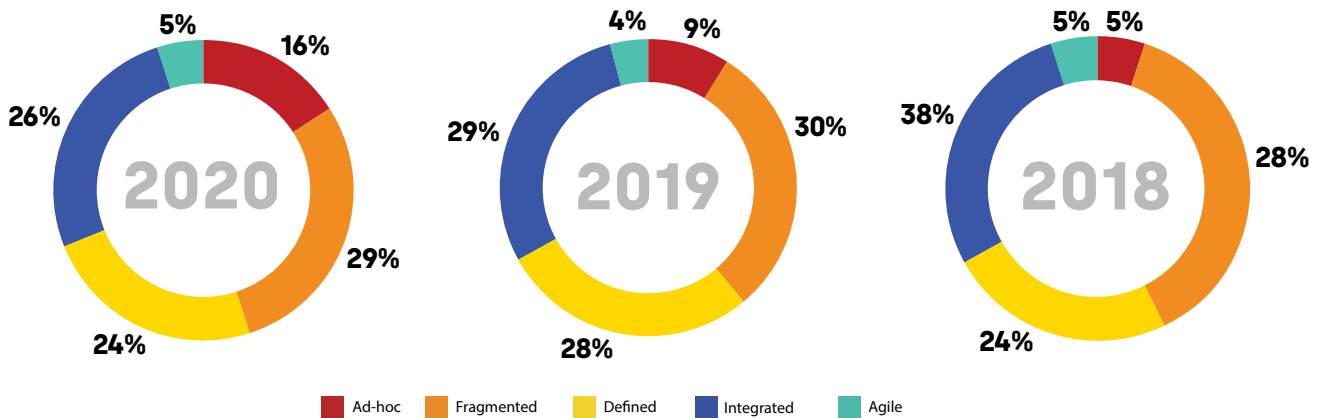
Board engagement and oversight is an important factor when it comes to advancing the maturity of programs. Organizations that had a high level of board oversight were much more likely to have programs in the Defined to Agile stages (69%) than those with low oversight (33%).

Program Maturity

Third-party risk programs are slow to mature, and there hasn't been any notable advancement in maturity across programs in the past three years.

A better understanding of maturity and the maturity stages, helps organizations recognize what to prioritize and focus on, where to invest and also what "not" to do.

The results revealed that there had not been any material advancement in the overall maturity of third-party risk management programs over the past three years.



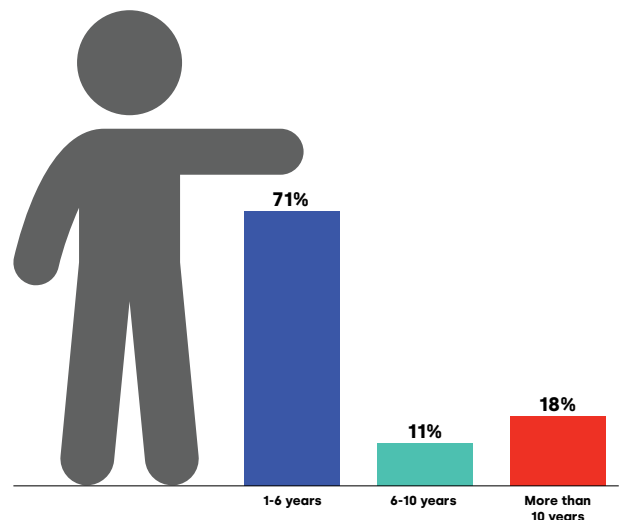
Maturity takes time.

Not surprisingly the longer a program has been in place, the more mature programs are likely to be. This year's survey revealed that 71% of programs are six years old or younger; 11% are between 6-10 years; and 18% have been in place more than 10 years.

Some programs get stuck.

What is concerning is that there are programs that are more than ten years old, existing at the Ad-hoc stage (8%) and the Fragmented stage (13%) after that period of time.

Lack of resource, lack of board engagement, and insufficient tools are all likely to play a part in this slow development.





Results

This section of the report sets out the results of the 2020 benchmarking survey. As this is the third year that the survey has been conducted, it also provides insight into 2018 and 2019 results where appropriate, to provide a view of year on year trends.

Part 1: Maturity and Age

At the center of many third-party risk management program conversations today is the concept of maturity. A better understanding of maturity and the maturity stages helps organizations recognize what to prioritize and focus on, where to invest, and also what “not” to do.

Within organizations, third-party risk management goes through a progression of stages that reflect the maturity of the program in its totality: the people, processes, governance, and technology. There are various frameworks for assessing maturity, but the most useful encompass five stages. The model used in this research, was defined in conjunction with leading industry expert, Michael Rasmussen of GRC 20/20, and identifies the stages as beginning at Ad-hoc, and progressing through Fragmented, Defined, Integrated, and Agile.

Initial/Ad-hoc: Siloed, ad hoc practices. No third-party risk framework, tools, or formal program. No third-party segmentation. Lack of skills and resourcing. No defined roles and responsibilities. No governance structure or third-party risk management authority matrix in place.

Developing/Fragmented: Starting to determine a roadmap, with pockets of good practice emerging. Basic segmentation in place and some standardization of on-boarding registration and qualification. Some areas of risk management are in place (e.g. ABAC, infosec), but are not approached in an integrated or structured way. Third-party risk management framework agreed but not implemented, with required skill sets identified. Some basic performance management. Governance and processes not fully embedded.

Defined: Third-party risk program and processes are defined with roles and responsibilities agreed. A formalized approach is in place with the framework designed and control practices in place. Risk appetite not yet well defined or aligned, although inherent risk assessments are maturing.

Established/Integrated: Governance model agreed at board level. Standardized third-party risk management approach implemented and adopted with documented processes. Third parties are segmented according to agreed and understood criteria. Robust performance measures are in place. Appropriate skill set and resources with roles and responsibilities allocated. Third parties engaged and involved.

Optimized/Agile: Comprehensive governance structure with periodic meetings with board and regular governance review meetings. Third-party risk appetite and thresholds well defined and understood. Segmentation reviewed annually. Cohesion across 3 Lines of Defense. Issue escalation rarely needed and resolved quickly/effectively. Able to identify areas of improvement and measure ROI for relationship reviews and continual improvement. Industry best practices understood and embraced. Enterprise view of third-party ecosystem risk, compliance and performance.

Third-party risk management is a discipline on a journey. Today, more programs remain at the early stages of maturity [Ad-hoc – Fragmented: 45%] than the latter [Integrated – Agile: 31%].

This year 16% of respondents indicated that their programs were as the Ad-hoc stage, 29% at the Fragmented stage, 24% at the Defined stage, 26% at the Integrated stage, and 5% reported that they had reached the Agile stage.

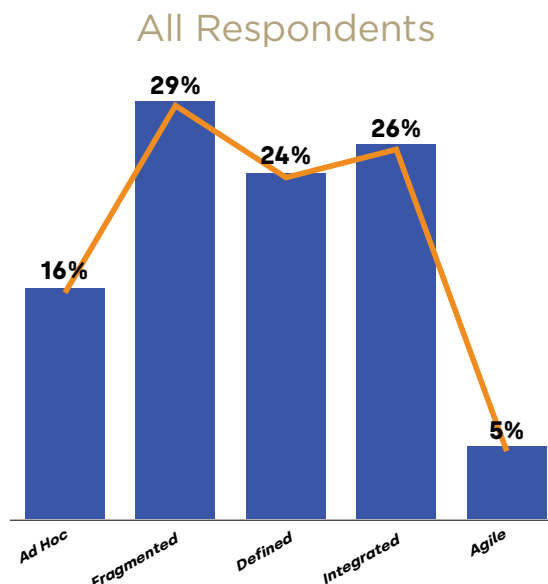


Chart 1: Which maturity level do you consider most closely describes your overall third-party risk management program?

Maturity has remained relatively static over the past three years.

Interestingly the greatest deviation between 2018 and 2020 numbers was at the 'Ad-hoc' stage where the proportion of respondees grew from 5% to 16%. This may be in part due to a greater proportion of non-financial services firms responding to the survey this year than in previous years. These organizations tend to have a lower maturity than those in financial services.

% of Respondents by Maturity Stage by Year

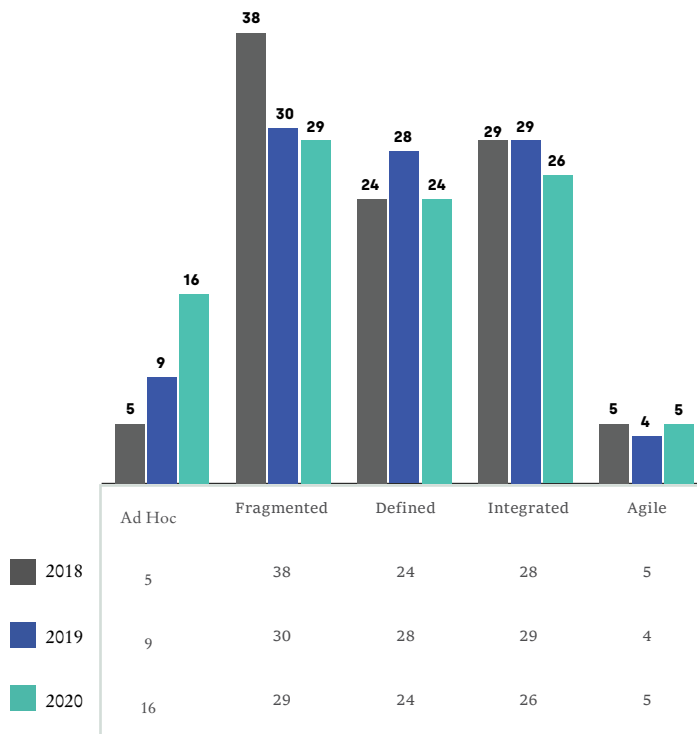


Chart 2: % of respondents by maturity stage by year

Financial services firms tend to be more advanced in their maturity levels than peers in other industries.

As a highly regulated industry, with a great deal of guidance and expectation set around third-party risk management, it should come as little surprise that respondents from financial services organizations reported a higher degree of maturity – with 37% in the Integrated to Agile range – than those respondents from non-financial services – 27% for the same range.

Financial Services

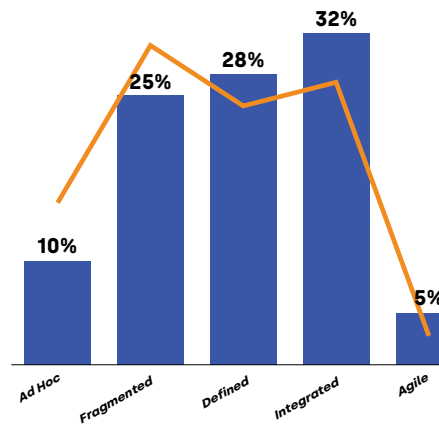


Chart 3: % of respondents from the financial services sector by maturity

Non-Financial Services

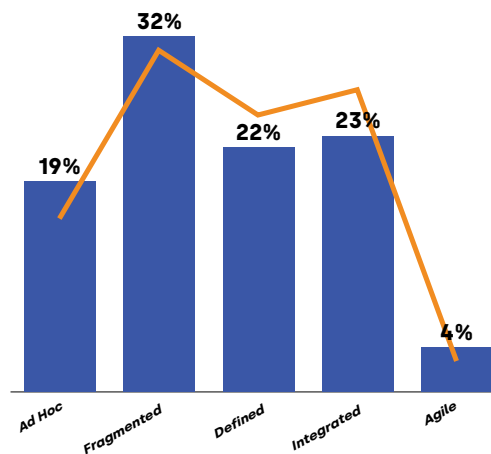


Chart 4: % of respondents from non-financial services sectors by maturity

Maturity takes time. Not surprisingly the longer a program has been in place – the more mature programs are likely to be.

Maturity is an important consideration, not least because third-party risk management as a discipline is relatively young. This year's survey revealed that 71% of programs are six years old or younger; 11% are between 6-10 years and 18% have been in place more than 10 years.

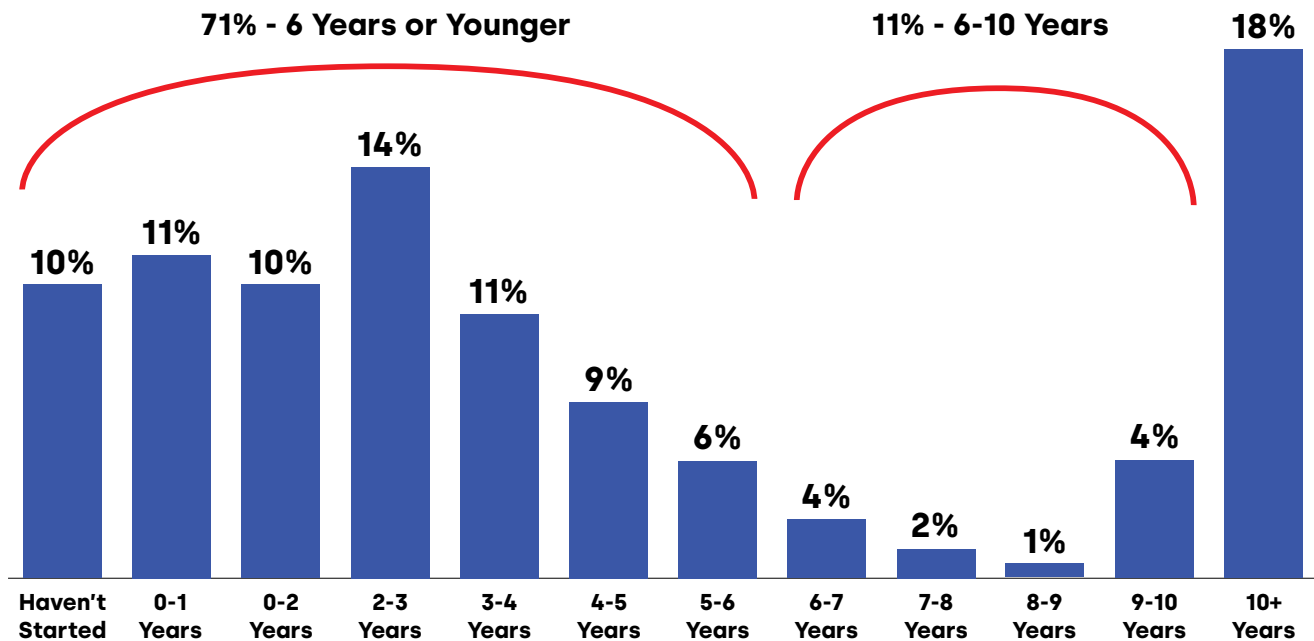


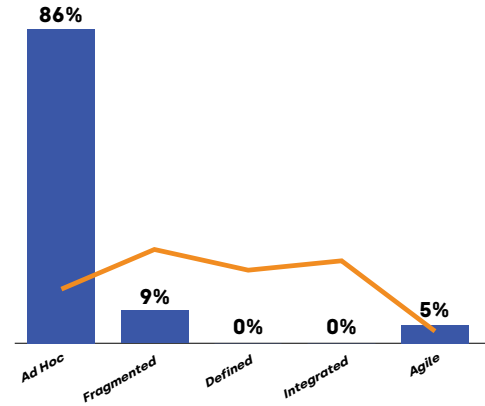
Chart 5: How long has your third-party risk management program been in place?

What is interesting about these results is that there are respondents whose programs are either not started or between 0-3 years, self-assessing that their programs are Agile (5% and 4% respectively). However, there are none between 3 and 10 years who report themselves as Agile. It's likely that reality has set in at this point of the journey, and there's a better understanding of how complex and multi-faceted programs can be and that there's still some way to go.

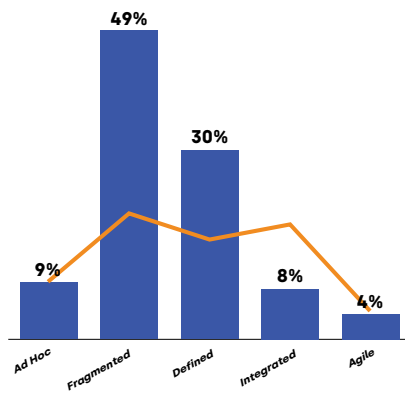
Some programs get stuck.

What is more concerning is programs that are more than ten years old existing at the ad-hoc stage (8%) and the fragmented stage (13%) after that period of time.

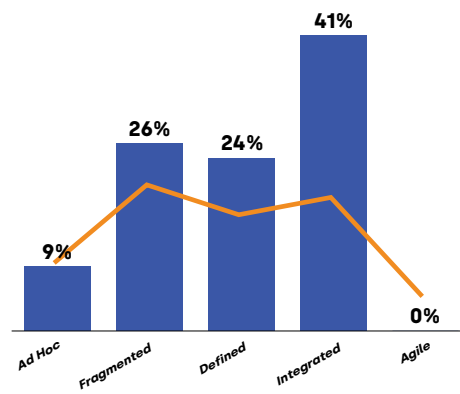
Not started



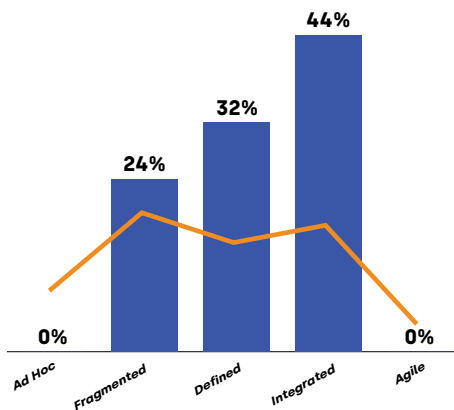
0-3 years



3-6 years



6-10 years



10+ years

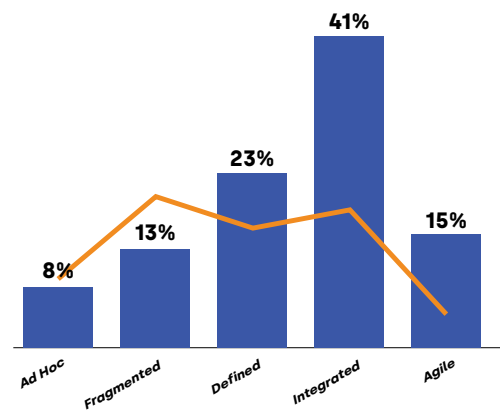


Chart 6: Maturity by age of program

Part 2: Third-Party Incidents

Third-party incidents that could damage the business are common.

Respondents were asked about whether there had been an incident associated with a third party in the last 12 months in their organization. Some respondents (21%) did not know if they had an incident.

Of those that did know, 59% had experienced at least one incident associated with a third party (some experienced more than one type of incident). This is down, somewhat, from last year's results which saw 75% of respondents reporting that they had experienced an incident.

Of these incidents – some translated into damage, others did not.

Had an incident associated with a third party that has caused significant business disruption and/or significant reputational damage	10%
Had an incident associated with a third party that had the potential to cause significant business disruption and/or significant reputational damage	21%
Had an incident associated with a third party that has caused some business disruption and/or some reputational damage	23%
Had an incident associated with a third party that had the potential to cause some business disruption and/or some reputational damage	33%
No incidents associated with third parties	41%

Table 1: Incidents and impact



CAUTION

In less mature programs, incidents are more likely to cause business disruption or reputational damage.

When you start to look at the breakdown by program maturity, some interesting trends emerge.

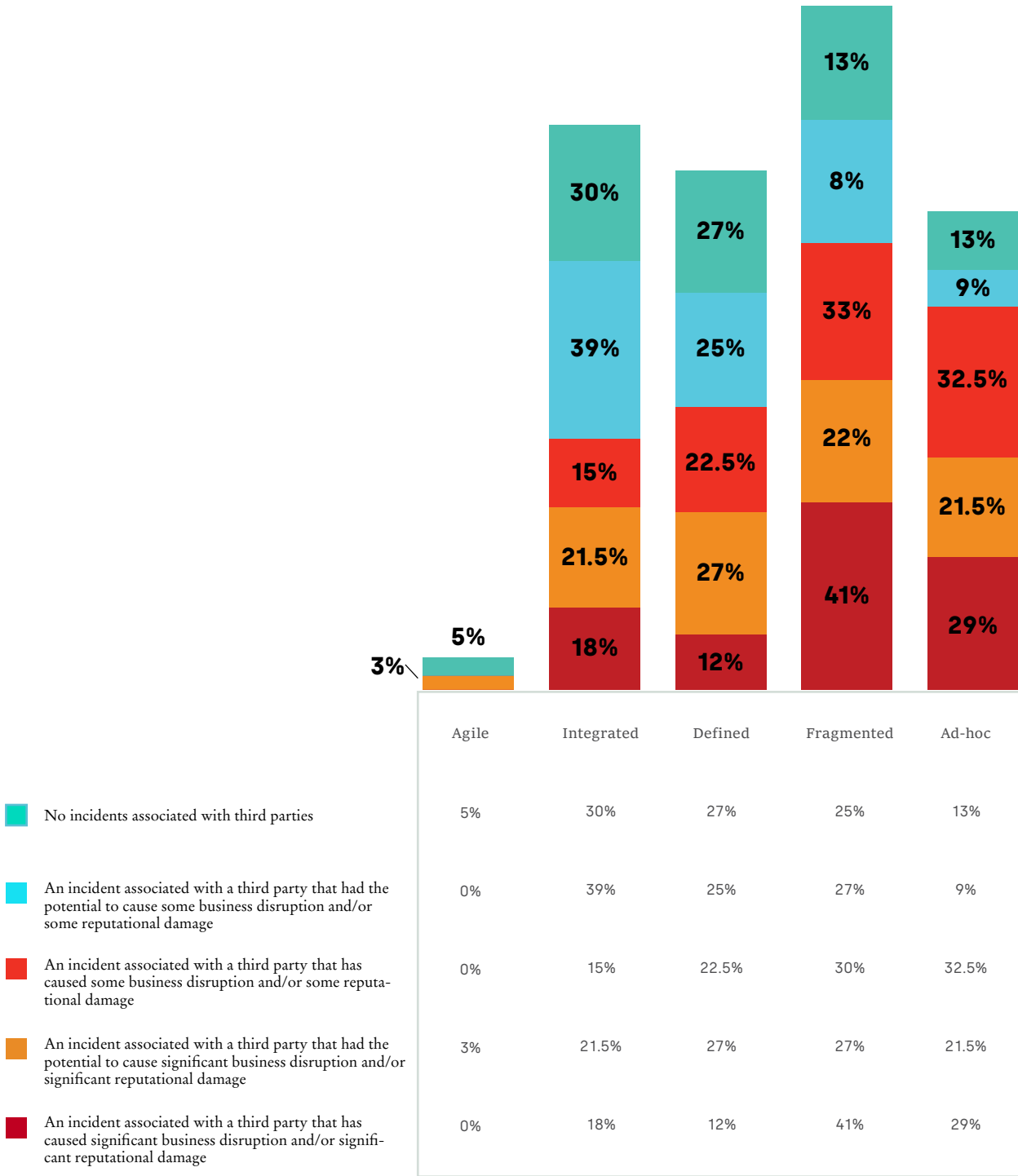


Chart 7: Incident impact by program maturity

Programs at both ends of the maturity spectrum were about equally as likely to report that they had not experienced any incidents with third parties (Ad-hoc – Fragmented 39%; Integrated to Agile = 34%).

However, when there were incidents, it appears that in less mature programs, incidents were more likely to result in business or reputational damage.

Incidents were more likely to cause significant business disruption or reputational damage in less mature programs (Ad-hoc – Fragmented 71%) than in mature programs (Integrated to Agile 18%).

Less mature programs also were more likely to experience incidents that caused some business disruption or reputational damage (Ad-hoc – Fragmented 63%; Integrated to Agile 15%).

These are important data points for third-party risk managers looking to build an internal business case for the value of a robust and mature program.

Performance and data breach incidents are the most common.

When dissecting the type of incidents that third parties had been associated with, 45% noted that they had experienced Performance/quality incidents, 22% Data breach, 21% Regulatory issues, 18% Cybersecurity incidents, 15% Continuity issues, 13% Financial, 12% Other, and 9% Legal.

Data breach	22%
Cybersecurity incident (hacked, malware, ransomware)	18%
Regulatory (e.g. ABAC non-compliance, GDPR non-compliance)	21%
Performance/quality	45%
Legal	9%
Financial	13%
Continuity (e.g. Third party went bust)	15%
Other (please specify the general nature)	12%

Table 2: Types of incidents experienced in the past 12 months.

The “other” types of incidents included:

“Development & Conversion Issues”, “Reputational”, “NCX”, “Corruption related”, “Security glitch that caused system to be down”, “Potential data loss”, “Vendor goes down, not sure of final cause. Impact minor”, “Life threatening injury resulting in system stand down”, “Vendor’s circuit connectivity failed”.

Part 3: The Board and Third-Party Risk

The board is a critical stakeholder in any TPRM program and engaging them in the right way – helping them to understand the strategic value that TPRM provides – requires good analysis and reporting.

Boards hold an important oversight function in third-party risk management. They need to understand their duty of care and ensure actions taken at the board meetings are properly documented to provide evidence that directors exercised their fiduciary duties.

Given good, actionable information, it's likely that boards will understand third-party risks more deeply. Boards also hold the power to ask the right questions of management about third-party risk and to ensure it has the right attention and resource in the organization.

A quarterly cadence of board reporting is typical.

This year, 14% of respondents did not know how often their organization reported to the board on third-party risk management matters. Of those that did know, 50% reported quarterly, 11% twice a year, 17% annually and 10% monthly. A further 12% did not report at all.

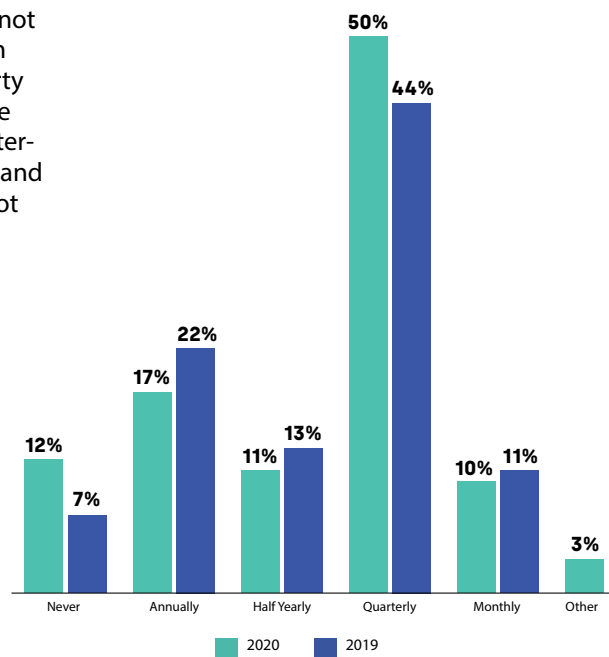


Chart 8: How frequently organizations report to the board on third-party risk by year

Cybersecurity continues to be the most pressing concern for boards, followed by reputational risks.

This year, as with last, cybersecurity (25%) and reputational risks (20%) were the most pressing concerns for boards. At the time of the survey, business resiliency in the event of COVID-19 was just beginning to emerge. Other risks boards were concerned about this year, included:

“Line of sight over critical suppliers”; “Transparent Accountability”; “Business resiliency - as a result of the coronavirus”; “Liability, IP Breach, Indemnity” and “GDPR compliance risks.”

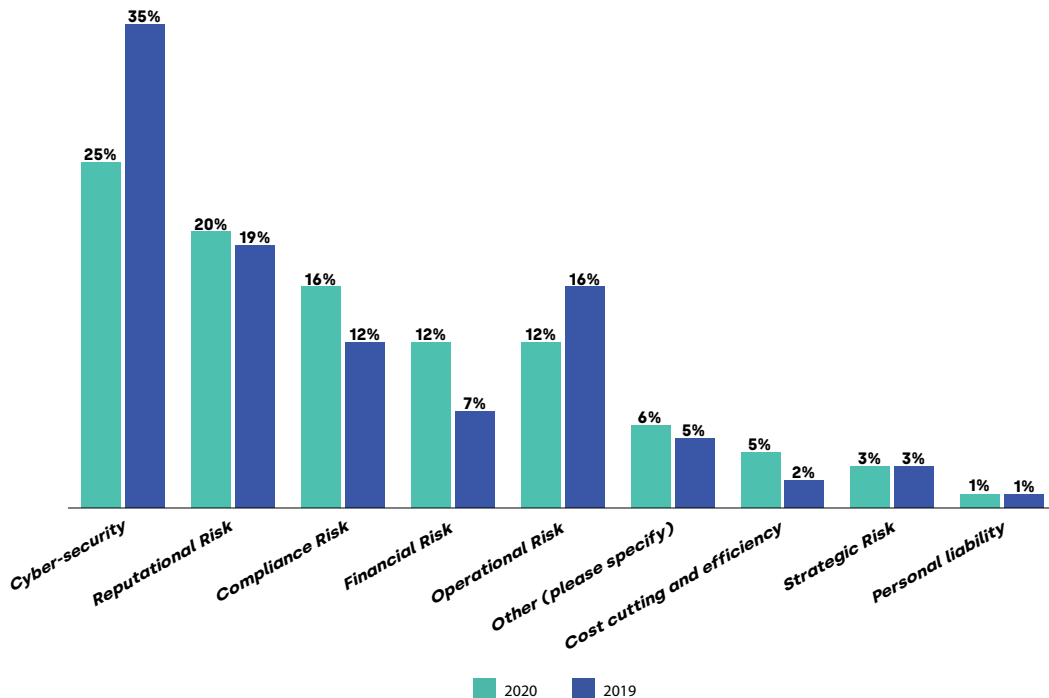


Chart 9: Top third-party risk related concerns for the board by year.

Many boards are not taking a leadership role in the governance of programs. Over a third of respondents (34%) reported that third-party risk management was not a key priority for their board, which provided only a low level of oversight.

Despite concerns across a broad range of risks, 13% of respondents stated that they did not know how engaged their board was. Of those that did, just over half (51%) reflected that their board had a moderate level of oversight, and 15% indicated that their board had a high level of oversight. This leaves more than a third (34%) that stated that third-party risk management was not a key priority for their board with only a low level of oversight.

It was surprising to see more boards with low engagement in this year’s survey, given the strategic importance of third parties to businesses and the risks that they expose the business to. The right level of oversight will, to a degree, be specific to the organization, the industry sector, and the size of the organization. But, when you consider that more than half of respondees (59%) had experienced at least one incident associated with a third party that either caused or had the potential to cause business disruption and/or reputational risk in the last 12 months, it may be a call for more boards to step up.

	2020	2019
High level of oversight – the board drive it and are actively engaged in reviews and alignment to corporate strategy.	15%	21%
Moderate level of oversight – our board are aware of it, they are notified of critical incidents, and they provide some governance.	51%	52%
Low level of oversight – Third-party risk management is not a key priority for our board.	34%	27%

Table 3: How would you categorize board engagement with your third-party program?

Too many boards don’t have a good handle on the third-party risks their organizations are exposed to.

In this environment of increased business risks, 40% of surveyed practitioners claimed that their board doesn’t have a good handle on third-party risk.

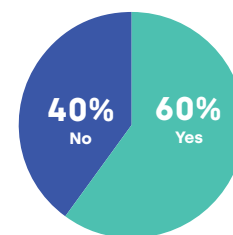


Chart 10: Generally speaking, do you think your board has a good handle on the third-party risks your organization is exposed to?

Having an engaged board is important to help advance program maturity.

The survey also dissected how board engagement impacted program maturity. This is an important vector, as to be successful, programs typically need some board and senior management sponsorship.

As the results reveal those respondents who indicated that their boards were moderately or highly engaged in program governance had significantly more mature programs than those whose boards had low engagement.

Organizations that had a high level of board oversight were much more likely to have programs in the Defined to Agile stages (66%) than those with low oversight (33%). Those with a moderate level of oversight had programs at these more advanced stages of maturity (64%).

High Board Engagement

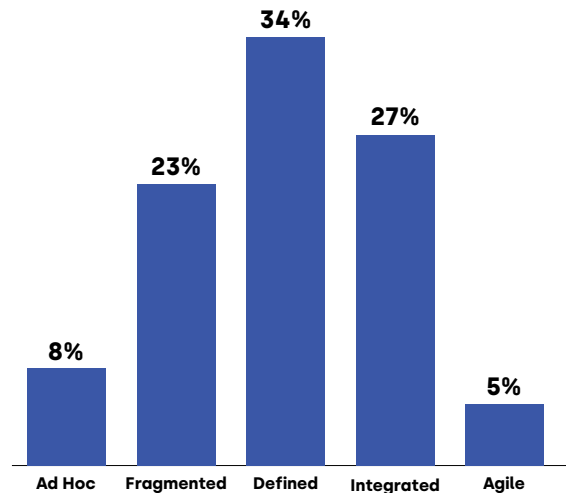


Chart 11: Maturity of programs in organizations reporting high board engagement

Moderate Board Engagement

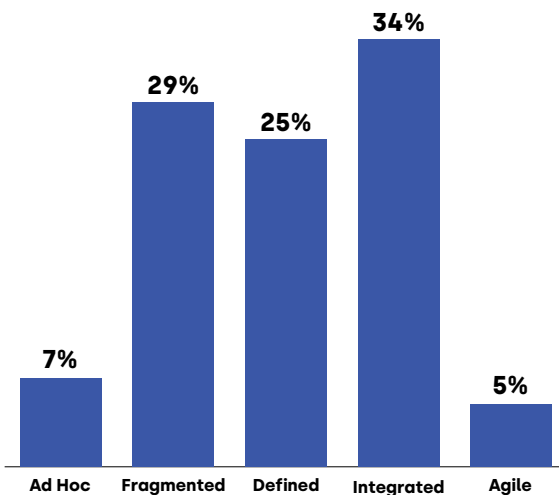


Chart 12: Maturity of programs in organizations reporting moderate board engagement

Low Board Engagement

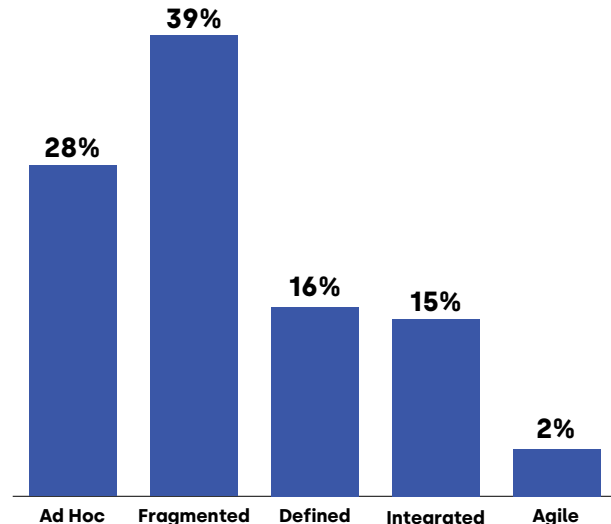


Chart 13: Maturity of programs in organizations reporting low board engagement

Part 4: Third-Party Risk Organizational Structure, Resource, and Budget

This section looks more closely at some of the operational practicalities that TPRM teams face today to understand the shape that these programs are taking and how they are being resourced.

There is a lack of consistent functional ownership of TPRM. Ownership shifts year-on-year.

There is no standardized functional structure for third-party risk management, yet there are many stakeholders involved in its management. This year we saw a sharp uptick in those organizations that situated third-party risk management under the compliance function, and a corresponding drop in operational risk. This is most likely due to this year's key constituent base due to the partnership with Compliance Week, and the fact that this year we saw a higher proportion of respondents from non-financial services organizations.

Typically, we see third-party risk management located under operational risk (or other risk functions), compliance, or procurement.

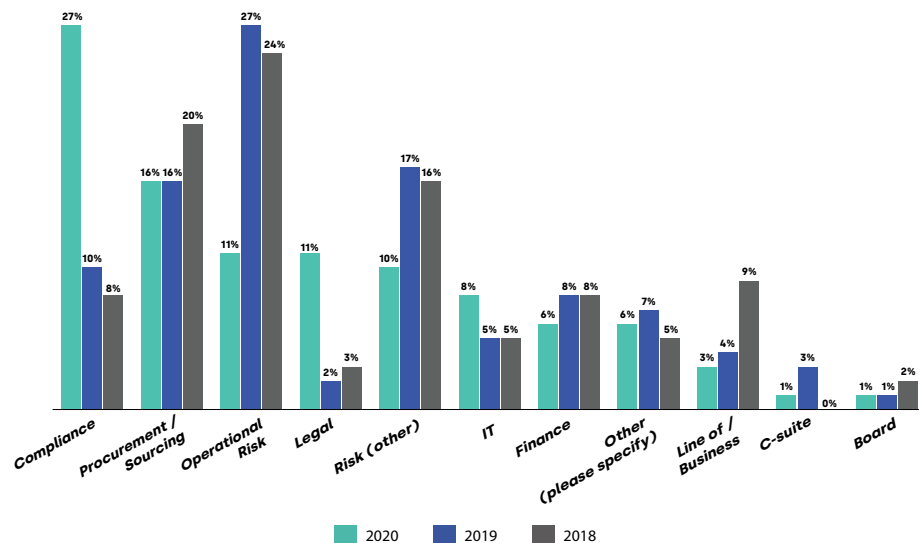


Chart 14: Under which function is third-party risk management primarily located and managed in your organization?

A centralized, in-house structure is the most dominant operating model for third-party risk management.

Close to half of organizations are adopting this model (45%), although there was an uptick, year on year for those companies favoring a decentralized, in-house model, from 14% in 2019 to 21% in 2020.

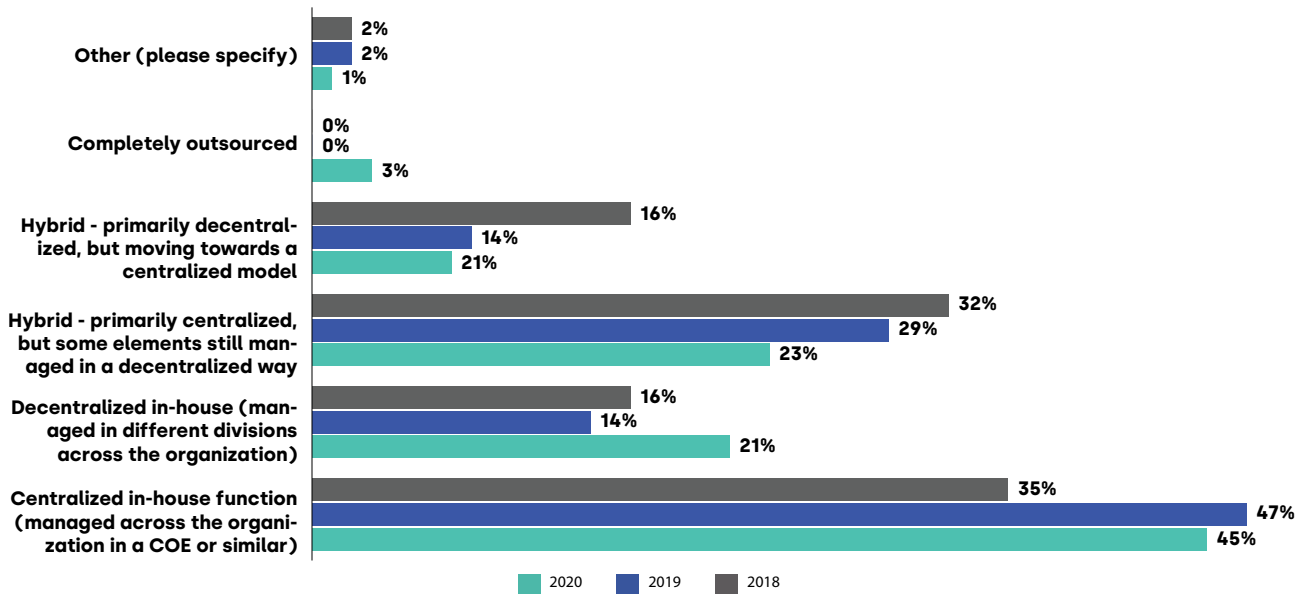


Chart 15: Third-party risk management in my organization is ...

Many organizations do not have a dedicated team to support third-party risk management, and when they do, they tend to be small.

Over a quarter of respondents (27%) indicated that they did not have a dedicated team to manage third-party risk at their organization, and 42% reported that their teams were between 1-5 people in size.

	2020	2019	2018
We don't have a dedicated team	27%	19%	26%
1-5	42%	47%	33%
6-10	13%	14%	14%
11-20	9%	7%	10%
20-30	5%	6%	6%
30-50	2%	4%	3%
>50	2%	3%	8%

Table 4: Size of team dedicated to third-party risk management

Organizations with no dedicated team or teams between 1-5 people are working with a significant number of third parties nonetheless.

When we drilled into how many third-parties were being managed with no dedicated team or small team sizes, the results were quite surprising.

More than half the respondees (60%) with no dedicated teams were still managing more than 500 third parties with 4% managing more than 50,000. This is an extraordinary amount of third parties to manage without a dedicated team.

Even for small teams, almost half (49%) were managing more than 500 third parties with 2% managing more than 50,000.

The lack of resource coverage here is alarming and something that organizations with small team sizes and large numbers of third parties should be looking to address. Automated technology and a risk-based approach will help, but people are an important success factor of any program.

How many third parties does your organization work with?

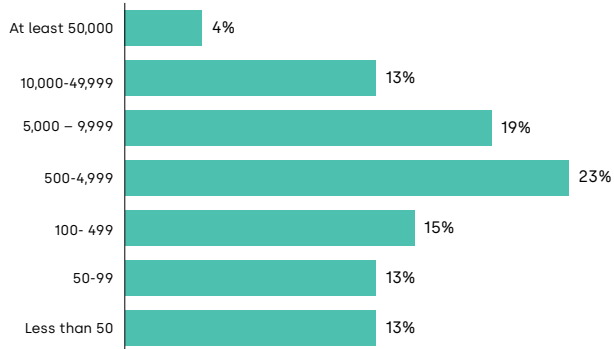


Chart 16: Number of third parties managed by organizations that don't have a dedicated team

How many third parties does your organization work with?

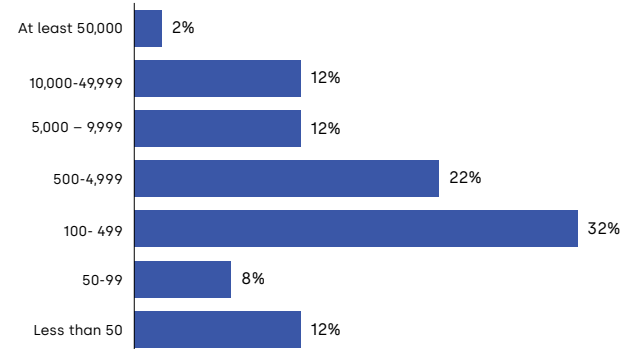


Chart 17: Number of third parties managed by organizations that have 1-5 dedicated team members

At least some of the heavy-lifting associated with TPRM processes is being supported by outsourcing.

This year, 29% of respondents said that they currently outsource some aspect of their third-party program, such as validation or due diligence, to shared service or managed service operations. Another 6% said although they were not doing so presently, they intended to do so in the future. These percentages are similar to previous years.

	2020	2019	2018
Yes	29%	31%	33%
No	55%	57%	53%
Not presently, but we intend to	6%	6%	8%
I don't know	10%	6%	6%

Table 5: Are you outsourcing any part of your TPRM processes to shared services or managed service operations? (E.g. validation, due diligence)

For such a complex and business-critical function, budgets remain relatively low.

As with prior years, a high proportion of respondents (40%) were uncertain of what budgets the organization had allocated for third-party risk management. Proportionally budgets remained relatively static year over year.

It's alarming that 6% of organizations had no budget for third-party risk management. A further 22% of organizations had budget, but no more than \$50,000. In addition, 28% had between \$50,000 and \$500,000 with only 4% having budgets larger than \$500,000.

Those with budgets larger than \$500,000 were from Financial Services (60%), Media and Communications (20%), Pharmaceutical (10%), and Technology (10%) companies.

	2020
I don't know	40%
\$0	6%
<\$5,000	8%
\$5,000-10,000	3%
\$10,000-50,000	11%
\$50,000-100,000	9%
\$100,000-250,000	12%
\$250,000-500,000	7%
\$500,000-1,000,000	2%
>\$1,000,000	2%

Table 6: Approximate budget (US\$) outside headcount for TPRM

Most third-party risk management program budgets are not going to grow in the next 12 months.

There's remarkable consistency year over year about budget status. This year 50% expected it to remain the same, 38% expected it to increase, and 12% decrease.

This survey took place before the full impact of COVID-19. When a crisis like this pandemic hits, generally there are a couple of likely outcomes for budgets: budgets are frozen for the immediate/foreseeable future due to uncertainty, or organizations expand/focus with renewed urgency into third-party risk and supply chain resilience due to the critical part these play in business continuity and operational resilience.

In the next 12 months I expect ...

Answer Choices	2020	2019	2018
Budget to decrease significantly	2%	2%	1%
Budget to decrease slightly	10%	9%	8%
Budget to remain the same	50%	53%	50%
Budget to increase slightly	32%	31%	35%
Budget to increase significantly	6%	5%	6%

Table 7: Over the next 12 months, do you expect to budgets to decrease/ remain the same/increase?

Around a third of programs are not getting the right level of resource to be successful.

Respondents were asked whether they felt they had the appropriate level of funding to support the people, tools, and innovation that is required for success in their third-party risk management program. As we have seen in previous year's responses around one third of respondents feel under resourced in each of these areas.

Do you consider your TPRM program has the right level of funding for:	1- Fully agree	2	3	4	5 - Fully disagree
The people (skill set and coverage) required to run your program successfully?	15%	24%	28%	23.5%	9.5%
The tools (technology and content sets) required to run your program successfully?	15%	21%	31%	25%	8%
Innovation and continuous improvements to your program?	14%	22%	31%	25%	8%

Table 8: Degree to which programs are funded adequately

Average salaries have decreased over three years.

Salaries can be helpful indicators of how the TPRM discipline is evolving, with a rising average salary a good indicator of the value that organizations place in TPRM skills.

Respondents were asked their total salary (base plus any bonus/benefits) and the currency for their salary figure. This enabled us to convert the salaries into US\$. It's important to keep in mind that this approach is fairly basic, statistically speaking. It does not take into account variables such as city location, years of experience, and other factors that can all play into compensation outcomes. However, by asking the question, it's hoped that it will provide an initial point for discussion and enable some analysis.

The lowest salary – \$6,300 – was for an advisor, working for a professional services firm in Mexico. The highest salary this year – \$850,000 – was held by a Chief Ethics & Compliance Officer, working for a technology firm in the US. The average global salary this year (\$137,547) is lower than the past two years' figures of \$159,600 (2019) and \$155,106 (2018).

Salary in \$US	Global	USA	UK/Ireland	Rest of Europe
High	850,000	850,000	163,928	386,250
Low	63,000	45,000	37,200	15,500
Average	137,547	157,031	98,460	120,974

Table 9: TPRM Salaries in \$US

Part 5: Third-Party Universe and Program

This section provides a lens into the programs of peers – how many third parties they work with, what proportion of these are critical and high risk, what kinds of risks are they monitoring, and the methodologies and technologies they are using.

Around a quarter of companies work with between 500-4,999 third parties, and just under 20% work with over 10,000.

Among survey respondents, 20% didn't know how many third parties their organization worked with.

Of those respondents that did know, it appears that many organizations continue to work with large numbers of third parties – 19% of respondents say they have 10,000 or more third-party relationships. Another 13% say they engage with between 5,000 and 9,999 third parties.

However, the largest percentage – 26% – say they have between 500 and 4,999 third-party relationships.

A significant number of organizations engage with a smaller number of third parties. Some 22% say they have between 100 and 499 third-party relationships, while almost 20% say they have 99 or fewer third parties.

	2020	2019
At least 50,000	6%	2%
10,000-49,999	13%	10%
5,000 – 9,999	13%	10%
500-4,999	26%	40%
100- 499	22%	20%
50-99	9%	4%
Less than 50	11%	14%

Table 10: How many third parties does your organization work with?

Almost half of organizations don't have all their third parties in a single inventory.

Of those who responded, 16% didn't whether they had all their third-parties accounted for in a single inventory or not.

The number of organizations who say they have a single inventory of all of their third parties declined from 60% in 2019 to 51%, in this year's survey.

For respondents who didn't have a single inventory, the survey asked what proportion of their third parties could be accounted for in a single place.

Of these 35% didn't know. Of those that did know (44%) had no more than half of their third parties' information maintained in a single inventory.

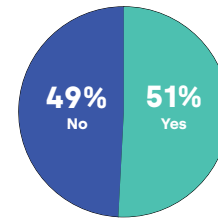


Chart 18: Do you have a single inventory of all your third parties?

0	5%
1-10	9%
11-30	20%
31-50	22%
51-70	22%
71-90	17%
91-99	5%

Table 11: If you answered "no", what percentage of your third parties are maintained in a single inventory?

Three quarters of organizations classify between 1-30% of their third parties as critical.

One quarter (25%) of respondents did not know what percentage of their third parties would be categorized as critical. Typically, organizations had between 1-10% of their third-party population deemed critical (43%). There were some organizations (11%) who indicated that over half their third-party universe were critical suppliers.

	2020	2019	2018
0	2%	-	4%
1-10	43%	59%	49%
11-30	32%	26%	29%
31-50	12%	6%	9%
51-70	5%	4%	5%
71-90	3%	1%	3%
91-99	1%	2%	-
All	2%	2%	1%

Table 12: What percentage of your third parties would you classify as "critical"?

Over three quarters of organizations classify 1-30% of their third parties as high risk.

Proportionally the results were very similar to the percentages deemed critical. One quarter (25%) of respondents did not know what percentage of their third parties are classified as high risk. Typically, organizations had between 1-10% of their third-party population categorized as high risk (42%). There were some organizations (8%) who indicated that over half their third-party universe were high risk.

	2020	2019	2018
0	2%	2%	5%
1-10	42%	42%	52%
11-30	35%	42%	33%
31-50	13%	9%	7%
51-70	5%	1%	1%
71-90	1%	1%	-
91-99	1%	2%	-
All	1%	1%	2%

Table 13: What percentage of your third parties would you classify as "high risk"?

Only a quarter of respondents say that all of their third-parties have undergone initial due diligence.

When asked, 22% didn't know what proportion of their third-party universe had undergone initial due diligence. Of those that did know, 4% admitted that none of their third parties had been subject to initial due diligence. Only one quarter had applied initial due diligence to all their third parties, with 44% applying initial due diligence to no more than half of their third parties.

Answer choices	2020	2019	2018
0	4%	2%	2%
1-10	17%	12%	13%
11-30	11%	9%	8%
31-50	13%	10%	9%
51-70	11%	7%	15%
71-90	12%	15%	18%
91-99	7%	15%	8%
All	25%	30%	27%

Table 14: What percentage of your third parties have had initial due diligence conducted?

The vast majority (83%) of respondents are not conducting ongoing monitoring or due diligence on all their third parties.

While 21% of respondents didn't know if they were conducting ongoing monitoring, of those that did know, only 17% reported that were applying this to all their third parties. Most (51%) reported that no more than half their universe of third parties were subject to ongoing monitoring/due diligence, and 8% conducted no ongoing on any of their third parties at all.

The US Department of Justice specifically calls out ongoing monitoring in its June 2020 update of the Evaluation of Corporate Compliance Programs.

“Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.”

Answer choices	2020	2019	2018
0	8%	2%	4%
1-10	25%	21%	25%
11-30	14%	18%	21%
31-50	12%	11%	12%
51-70	9%	11%	6%
71-90	9%	6%	11%
91-99	6%	7%	4%
All	17%	24%	17%

Table 15: What percentage of your third parties have ongoing monitoring /due diligence conducted?

Overall, contract reviews and renewal remain the most utilized practice in third-party risk management, followed by due diligence and risk assessments.

Many other best practices, including performance reviews, issue management, and corrective actions are not being used, suggesting a focus on the onboarding part of the relationship, rather than the full lifecycle.

While more than half of respondents were utilizing contract renewal, due diligence, risk assessments, and the onboarding processes to help manage third parties, less than half were adopting performance reviews, issue management, corrective actions, vendor self-assessments, performance scorecards, or site visits.

For those selecting 'Other', the types of processes they also embedded in their program were: *“financial due diligence”, “financial and security assessments”, “annual credit review”, “certifications”, “peer banking experiences with the vendor”, “training”, “on site business reviews to our headquarters”, “cyber alert monitoring”, “termination”, “IS performance scorecards for Mission Critical & Highs”, audits.”*

Contract review/renewal	82%
Due diligence	70%
Risk assessment	66%
On-boarding process	62%
Performance reviews	38%
Issue management	37%
Corrective actions	30%
Vendor self-assessments	29%
Performance scorecards	32%
Site visits	33%
Other (please specify)	7%

Table 16: Which of the following processes does your organization use to manage your third parties

Cyber risk, data privacy, and compliance/regulatory risk are the leading risks being managed, but what is more revealing is the proportion of programs not managing key risks that third parties can expose organizations to.

The results illustrate the risk management gaps in many programs. They reveal a third or more of programs are not managing for cyber risk, data privacy, and compliance and regulatory risk. Only around half are factoring in reputational and operational risk. Fewer than half of respondents are managing for the remaining broad range of risk types.

Cyber risk/ information security risk	67%	Country/geographic risk	34%
Data privacy	63%	AML	31%
Compliance risk/regulatory risk	62%	Credit risk	31%
Reputational risk	52%	Customer risks	30%
Operational risk	52%	Strategic risk	27%
Business continuity risk	49%	Human resources risk	26%
Fraud risk	43%	ABAC	21%
Physical security	41%	Market risk	19%
Internal controls risks	39%	Concentration risk	17%
Financial viability risk	38%	Other	1%

Table 17: What risk types are managed in your third-party program? (check all that apply)

Many programs still have a way to go when it comes to ensuring best practices are entrenched.

The responses to this part of the survey (which excluded those respondents who 'did not know') serve to highlight the gaps in programs today. Many of these gaps not only expose the company to risk, but would also be seen as compliance program failures in the eyes of the regulators.

Fewer than half of respondents could answer with confidence that they require a risk assessment for all new third parties pre-contract (46%). While some said they would do this partially, 14% reported that do not require this in their programs.

Companies are also failing to manage the full lifecycle of risk in their programs, with only 35% reporting that they do this completely.

This has regulatory implications with the DOJ’s June 2020 update of the Evaluation of Corporate Compliance Programs providing guidance for prosecutors to assess: “Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?”

Companies are also failing to apply programs consistently across all lines of business, with only 42% responding that they do this fully.

Business continuity is another area that is failing to be incorporated into programs, with only 46% of respondents indicating that this was fully factored into programs. In the current climate, operational resilience, supply chain resilience, and business continuity are all going to become increasingly important in third-party management, and are other areas for programs to improve.

Only 45% of respondents felt that their third-party risk program is fully aligned to the risk appetite of their organization. Third-party risk appetite is the level of risk resulting from relationships with third parties that the organization is willing to take in pursuit of its strategic objectives. This could mean that many organizations are taking on more risky third-party relationships than they are strategically willing to take or closing doors on opportunities that they could have pursued.

Fourth party risk is another area of exposure, with only 32% of respondents indicating that they have full requirements for their third parties to identify their sub-contractors/providers, with another 36% indicating they do this on a partial basis. A further 45% do no due diligence on their critical fourth parties.

Finally, few organizations have robust exit plans in place for critical third parties. Only 36% responded with confidence that they have full plans in place.

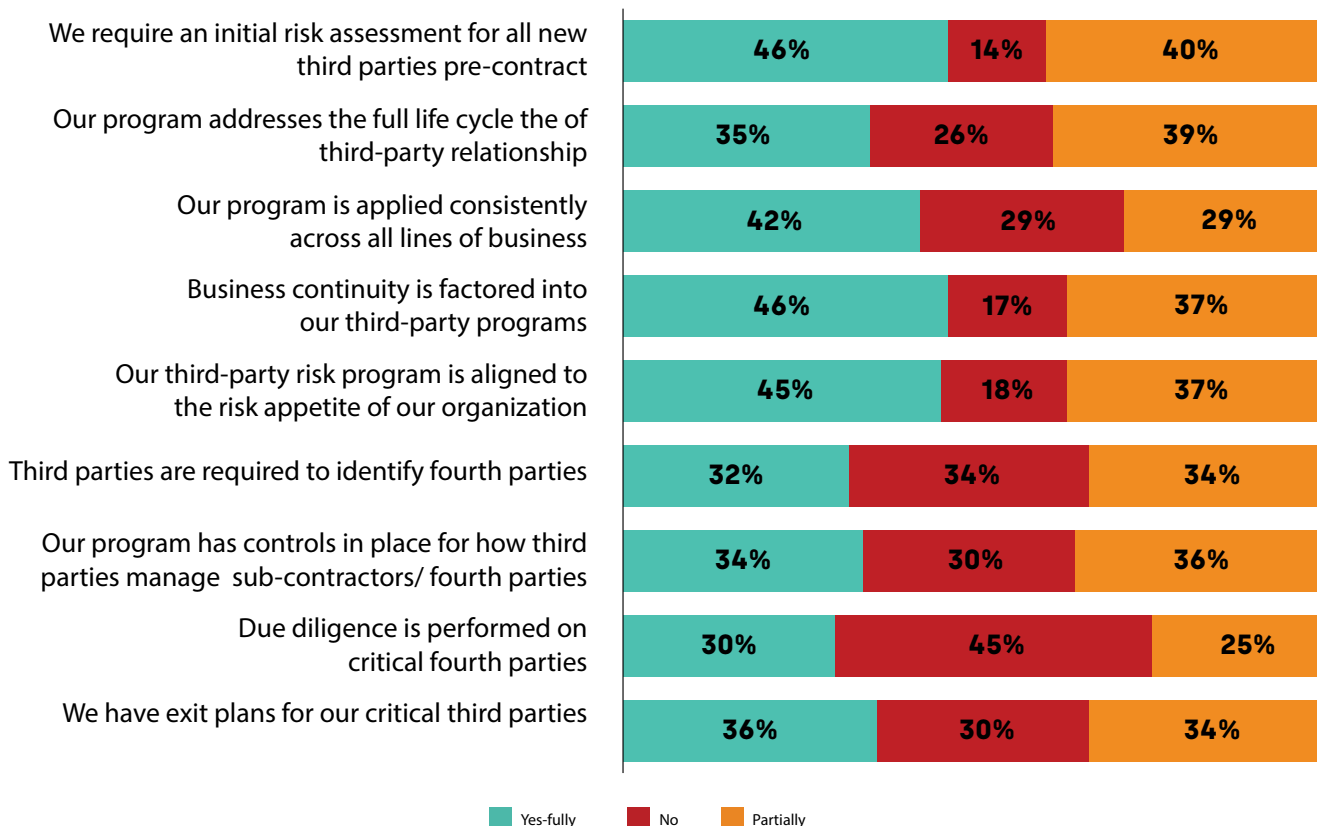


Chart 19: Please indicate which of these statements reflects the third-party program you have in place in your organization

The ability to report on key third-party program metrics is a challenge for most organizations.

Reporting was another area that highlighted key areas for improvement in third-party programs (and the technology choices made to support them).

Only 20% of respondents indicated they could report “*completely and quickly*” on the most basic of data points – what third parties they have. A slightly higher proportion (30%) could do this for critical third parties and third parties with the highest degree of inherent risk.

Over two thirds (67%) would struggle to report with any degree of confidence and efficiency on non-compliant third parties, with 11% revealing that this would be impossible.

Companies would also struggle to understand what third-parties have breaches or incidents associated with them – only 18% could provide a report on this important data point completely and quickly.

	Completely and quickly	Completely but would take some time	Partially and quickly	Partially and would take some time	Impossible
All third parties	20%	24%	20%	28%	8%
All critical third parties	30%	23%	17%	27%	3%
Third parties with the highest level of inherent risk	29%	22%	17%	25%	7%
Third parties with the highest level of residual risk	26%	21%	18%	26%	9%
Non-compliant third parties	22%	17%	17%	33%	11%
Third parties with breaches or incidents	18%	22%	15%	36%	9%
Third-party risk scorecard/ profile across all applicable risk and performance domains	15%	21%	18%	27%	19%
Third parties with remediation plans underway	13%	22%	19%	31%	15%
Third parties with cyber-risk exposure	18%	23%	17%	27%	15%

Table 18: Please indicate how easy it is to report on the following in your program

Part 6: Technology

This section of the survey looked at technology choices and the challenges that organizations were facing with technology.

Over a third of programs (34%) are still relying on spreadsheets and manual processes.

Some of the challenges associated with reporting likely lie in the primary technology that organizations are using to manage programs. Over a third of programs (34%) are still relying on spreadsheets and manual processes, and 17% are relying on an in-house system. Only 20% are using a specialist third-party risk management solution.

Spreadsheets/manual	34%
Specialist third-party risk management solution	20%
In-house system	17%
GRC platform	16%
ERP system	9%
Outsourced service	4%

Table 19: What technology/tools does your firm use to track and manage your third-party risk processes?

Greatest technology challenges

Respondents were asked an open-ended question: “What are your greatest technology challenges?” These were then grouped by theme and the number of mentions noted. Respondees could relate to several challenges in the one response.

The three most common technology challenges, related to limitations in the capabilities of their current system/s, adoption and buy in from internal stake holders, and data accuracy and reporting.

The capabilities of current technology systems are considered the biggest challenge this year by a considerable margin.

Capabilities of the current system. Respondents are growing increasingly frustrated by outdated, inefficient, and inflexible tools to manage third-party risk. They spoke of the difficulties they were having with adapting their current software tools to the evolving demands of the discipline. This was the top challenge for the last two years as well – and it's clear that dated, legacy technology remains a significant issue for TPRM teams.

A snapshot of responses on this theme include:

"Data inaccuracies, workflow capabilities, inability to integrate with other systems, systems designed to be centrally managed rather than self-service."

"Too broad/generic...not too easy to customize."

"Programming to capture desired workflow."

"Knowing what the non-compliance points, from past years, are at a glance. And also analyzing third parties, and regions, based on compliance and non-compliant issues."

"We don't currently have a single source of record for all vendors. Pulling inventories based on the type of work done is nearly impossible."

"Internally built system does not naturally have built-in capabilities of purpose-built systems, requiring enhancement / development and resulting in inefficiency in delivery of the program (manual processes, errors in the system, etc.)."

"Customizing tool to meet our specific needs. Training stakeholders to use tool properly."

Cultural challenges - adoption, buy-in and internal challenges gained prominence this year. Concerns with a general lack of understanding of risk and process, coupled with concerns associated with training and adoption featured in this theme.

A snapshot of responses on this theme include:

"Moving from spreadsheets to Third-party Management Tool Platform (TP immaturity and some not understanding benefits of moving to a centralized, integrated GRC Module)."

"Not enough risk awareness and necessary countermeasure recognition."

"SME training and usage - they aren't in it daily so they forget or let their passwords expire."

"Conversions of key systems to new systems. General employee understanding for timely notification and response and employee patience when systems not available. Getting adequate financial budgetary support to keep current."

"Getting all of our people to use it."

Data accuracy and reporting. Respondees again this year called out a lack of confidence in their data and reporting. It was clear that this was closely related to frustrations associated with disparate systems and not having a single version of the truth.

A snapshot of responses on this theme include:

"Incomplete / Inaccurate data in the ERP system as well as decentralized Vendor Master Files of divisions not on the same ERP system."

"We don't current have a single source of record for all vendors. Pulling inventories based on the type of work done is nearly impossible."

"Ensuring the integrity of the data in our vendor universe."

"Reporting and dashboards."

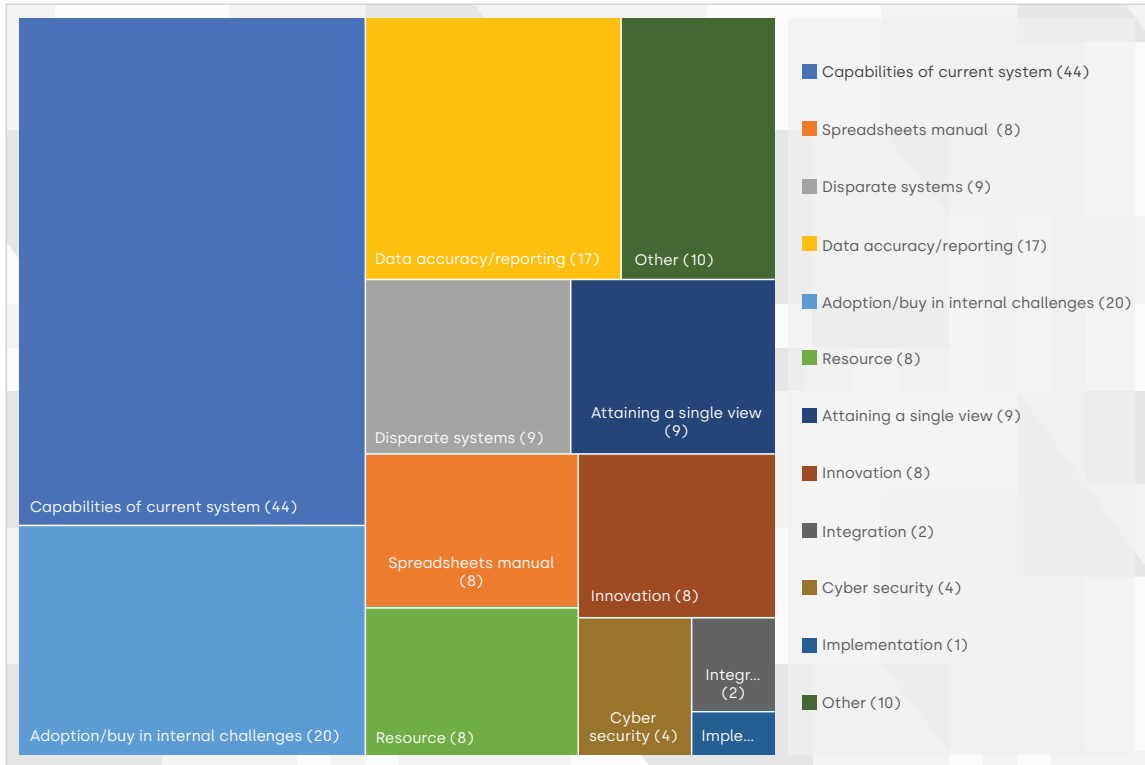


Chart 20: Greatest technology challenges by theme

Part 7: Challenges and Opportunities

This section provided respondents the opportunity to express in their words what they saw as the greatest challenges and opportunities for third-party risk management in their organization in the year ahead. Responses were grouped by broad themes, and the number of mentions noted.

Challenges

The most commonly mentioned challenges related to delivering best practice, specific risk types, and resourcing.

Delivering best practices. Given the limitations in programs that were exposed in the more quantitative questions in the survey, it's not a surprise that this issue has come up with the most frequency when respondents were asked about their challenges in a more qualitative way. What this theme tended to accentuate is that respondees are aware of and want to deliver best practice, but that this was not necessarily an easy process. Core elements of managing risk through the lifecycle of the relationship were called out as challenges.

From the very basic:

"Ensuring all third parties are accounted for",
"to draft a third-party risk mgmt. program or policy",
"Issuing and enforcing a consistent policy".

To the more standard and advanced:

"Enhancement of due diligence process and risk assessment",

"Inventorying, evaluating, and risk ranking important 3rd parties",

"Being able to have a holistic approach together with a systematic way to perform due diligence and assess results on an ongoing basis."

"Proper and standard approach to all levels of risk assessment.

"Identification of Fourth parties. Building practical GDPR and Cyber clauses into all contracts."

"Rolling out new automated platform, increase due diligence scope to low risk third-parties." "Monitoring 4th party vendors, managing Ongoing Monitoring, developing vendor concentration reporting and vendor spend monitoring."

"1. expanding the scope of risks addressed to include reputational, compliance, financial in a real time/continuous manner. 2. ensuring expanding scope of third parties are assimilated into program e.g: Brokers".

Specific risk types. As revealed in the quantitative section of the survey, organizations are managing a wide range of risks. The challenges associated with these, in particular cyber security, were also called out as challenges for programs in the 12 months ahead.

Cybersecurity. Of the risks that were mentioned, cyber security and data security, stood out with 68% of mentions. A snapshot of some of the responses referencing cyber security, include:

"Cybersecurity and dependence on other suppliers in the chain",

"Cyber security, privacy, data protection, concentration risk, performance management, cost savings", "Cyber compliance",

"Cybersecurity upkeep",

"Data breach";

"Evolving data security requirements",

"Hacker's activity".

Concentration risk. This challenge had elevated presence this year. A snapshot of some of the responses referencing concentration risk include:

“Managing the growing number of cloud vendors and being prepared for concentration risk based on limited number of cloud providers servicing multiple TSPs”,

“cyber security, privacy, data protection, concentration risk, performance management, cost savings”,

“Risk concentration”,

“Fourth Party Concentration Risk; Utility Concentration Risk”.

Resources. Adequate resourcing is an ongoing challenge for the nascent third-party risk management discipline. There is a succinctly expressed regulatory expectation for compliance programs to be “adequately resourced and empowered” yet many respondents mentioned the lack of resource to do the job properly, with typical responses including:

“Lack of staff to do a more thorough job”

“Lack of budget. Shrinking appetite for associated administrative burden considering no suppliers have been ‘Denied’ to this point”

“Having enough people to properly manage Third-party risk”

“Being able to manage the amount of oversight and due diligence needed with limited number of resources”

“Obtaining necessary resources to bring program up to industry best practice”

“Getting budget to install and use a tool”,

“Increased level of regulatory expectations without commensurate increase in resources/\$”

Others also specifically mentioned the challenge associated with getting senior management to understand the level of effort and budget required for third-party risk management:

"Convincing management of the need for more resources"

"Budget and support from C-suite"; "Human Capital and Management Buy-In"

"Getting Management to understand the work required to meet the Board's expectations"

"Getting buy-in from the line managers on the importance and the associated costs of due diligence".

Beyond third parties. Awareness that third-party risk management programs need to extend into managing the risk associated with fourth parties and Nth parties is growing, but organizations face real challenges when it comes to the operational reality of identifying and managing these.

"Identifying and monitoring 4th party risk"

"4th parties such as Cloud"

"Proper and standard approach to all levels of risk assessment. Identification of Fourth parties. Building practical GDPR and Cyber clauses into all contracts"

"Looking further into 4th party risk"

"4th party relationships"

"4th party oversight"

"Monitoring 4th party vendors, managing Ongoing Monitoring, developing vendor concentration reporting and vendor spend monitoring."

Other challenges that respondents cited in this open-ended question included:

Technology. These comments echoed many of those made in the tech challenges section. Specifically, comments pointed to the challenges involved in finding and implementing the right technology.

"Putting a system in place that is user friendly and has all the requirements to manage Third-party risk"

"Appropriately implementing the ERP system currently in the build phase for Third-party risk management"

Regulators and Regulations. Increased regulation was also regarded as a challenge.

"State regulation"

"cyber security & regulatory Compliance"

"increased level of regulatory expectations without commensurate increase in resources/\$"

"Increasing Regulation"

Scale and speed of change. Typically the number of third parties now having to be managed, and expanding existing programs were the challenges here.

"More third parties are being onboarded, resources & tools required to manage the spike"

"As we enter into more markets, intermediaries & third-party risk increases, we will likely have more intermediaries & third-parties to conduct risk assessments against."

Holistic view. Organizations are struggling to develop an integrated view of the risks that could cause significant disruption and/or reputational damage to the organization.

"Being able to have a holistic approach together with a systematic way to perform due diligence and assess results on an ongoing basis."

Resilience and continuity. Not surprisingly, given when the survey was live (Feb-March 2020), pandemic references were emerging in comments regarding continuity and resilience.

"Pandemic plan execution for third and fourth parties"

"Risk assessment for pandemic situations"

"business resiliency and quantification of risk"

Supplier participation. The ability to get suppliers actively engaged in programs was another issue some mentioned in their comments.

"We always have issues for supplier participation in risk audit"

"Educating third parties about the reporting requirements, when and how, and their responsibilities in keeping us apprised of significant issues."

Other challenges. These included an evolving threat landscape, keeping up to date, unauthorized people accessing systems, and reducing the number of international partners.

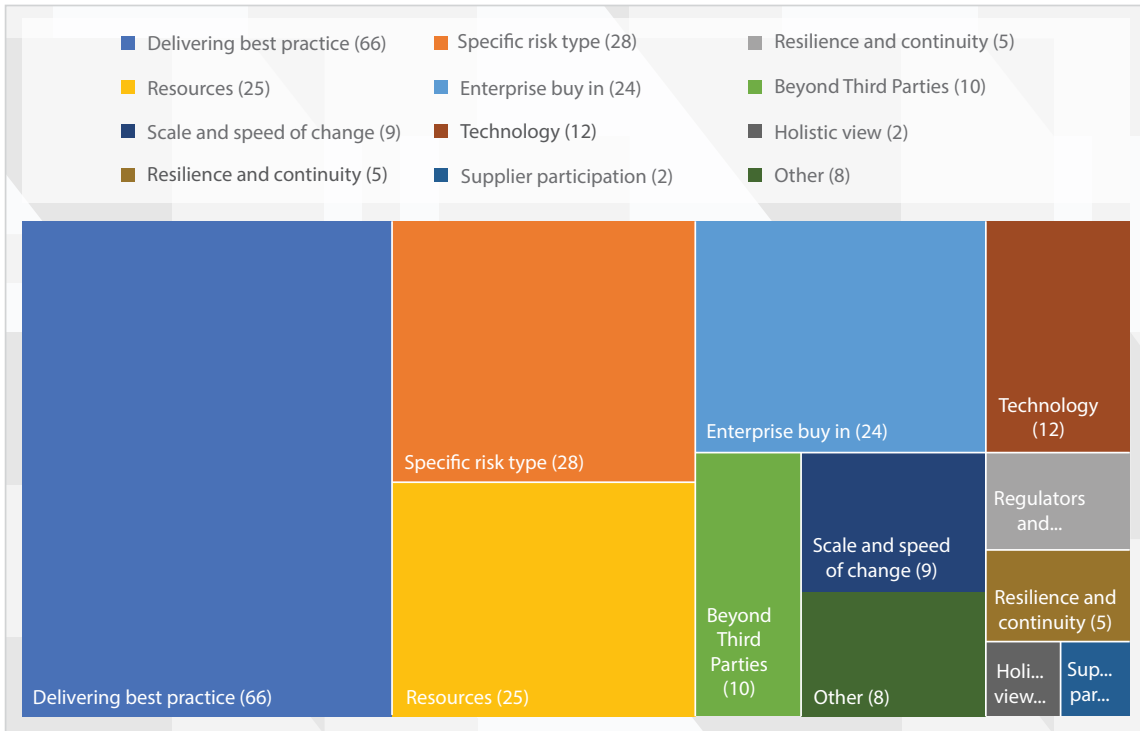


Chart 21: Greatest challenges for third-party risk management in the 12 months ahead by theme

Opportunities

The survey also sought to draw out what respondents saw as the greatest opportunities for third-party risk management within their organizations. These were wide and varied.

Improved processes. Respondents are looking to make real tangible gains in the everyday processes that their business and third parties have to use, such as processes for onboarding new third parties and conducting supplier due diligence.

These ranged from just getting a valid program off the ground:

"Putting in place such a program"

"Starting from beginning"

"Actually developing a comprehensive program from scratch"

"We will start a program to some extent"

"To draft a third-party risk mgmt. program or policy"

To creating more centralized processes:

"Centralized Risk Register"

"Build a more centralized process for Third-party risk management"

"Getting all third-party types on board, organizational buy in at all levels including the lowest levels (good high level buy in exists)"

"Centralized oversight."

To various process and operational efficiencies:

"Reduction of third parties with overlapping services, performance management, reduction of overall risk"

"Streamlining process....automated integration with contract management system to eliminate human error component, Increase in efficiency and structure"

"Integrating with other risk functions"

"Consolidation of risk, operational efficiency in managing 3rd party services, reduced compliance and reputational risks"

"Consistency across business and global contract management system"

"Continue to add more data into a global reporting application/system to identify relationships, any risks, and put mitigation plans into place"

"Sharing information among different business functions of the company and being more transparent"; "More streamlined processes"

"Streamlining new vendor reviews"

"Continued improvement on our onboarding process"

"Efficiency enabled by technology in streamlining delivery of the TPRM program ... removing workload on Third-party managers while also increasing the quality of evidence."

To outsourcing:

"Outsourcing risk management and associated deliverables, e.g. third-party master data updates, certificate renewals/management etc. to a third party."

The ability to mature programs was also raised by some as an opportunity for the year ahead:

"Maturing our processes"

"Developing an enterprise TPRM Policy / Standards for the organization to use to mature our current level of maturity in this area"

"Additional KRIs; continued maturity".

Better technology. Many respondents saw their most significant opportunities lying in better technology. Here they mentioned better automation, the benefits of a single platform, and better insight and reporting supported by technology:

"More opportunities and reasons to move to a fully electronic platform"

"Moving to a single platform"

"Streamlining process automated integration with contract management system to eliminate human error component"

"Tool to manage the third parties; risk assessment; mitigation plan"

"Platform to centrally manage and track that gives a dashboard of outside factors that's predictive and easy to use"

"New tools to support the due-diligence process"

"Continue to add more data into a global reporting application/system to identify relationships, any risks, and put mitigation plans into place"

"Deeper integrations, AI."

Improved culture and buy-in. Respondee saw a range of opportunities for third-party risk programs to benefit (and benefit from) business culture and buy-in across all levels of the organization.

From management:

"Upper level interest in compliance and risk mgmt will allow us to focus on and improve existing compliance functions, including 3rd party checks/audits"

"Inform decision making and bring visibility of third-party risk to the Board"

"Big disastrous events wake up the top management"

From the more operational stakeholders across the business:

"Getting all third-party types on board, organizational buy in at all levels including the lowest levels (good high level buy in exists)"

"Creating a transparent due diligence process, which will empower line managers to be part of the process"

"Greater focus by the company"

"Redesigning processes to make them more efficient and well received from the lines of business"

"Stakeholder engagement".

And by the third parties and suppliers themselves:

"Regulatory push is allowing us to ask for more due diligence items and processes from Third-party processors."

They also saw opportunities in better alignment and transparency:

"Opportunities to continue to socialize our program and obtain better alignment with model risk and AML risk programs"

"Sharing information among different business functions of the company and being more transparent."

And the ability to secure the appropriate resource in the process: "Grow the legal dept include new employees with the right background and experience."

Respondents also mentioned opportunities that related to:

Better data and reporting:

"...the ability to have useful metrics and dashboards,"

"Quantification of risk - today's Third-party software packages provide meaningless information to assess risk. We need probability loss distributions so senior executives can really understand risk, not single point heat maps that intersect likelihood an impact. Providing insight will be the key to being able to remediate vulnerabilities prior to the occurrence of a risk event."

"Advancement in analytics used for direct and direct procurement spending, organizational structure and working capital."

"As we understand our environment, our greatest opportunity will be in reporting and analysis of the data we develop."

Rationalization, cost-savings and efficiency:

"Reduction of third parties with overlapping services, performance management, reduction of overall risk",
"potential consolidation of vendors",
"cost savings",
"Efficiency enabled by technology in streamlining delivery of the TPRM program ... removing workload on Third-party managers while also increasing the quality of evidence",
"Getting the business to streamline the partners".

Having a holistic, single view of third parties:

"Having a comprehensive TP Risk Analysis and Management Platform covering all value chain",
"Holistic view of risk reviews",
"single pane of glass view of risk for vendors."

Industry standardization:

"Partnership with companies to share successful strategy/process",
"Industry support",
"Shared compliance testing".

Other: Some of those falling in the 'other' category, saw no new opportunities whatsoever, others saw opportunities associated with business growth and increased regulatory requirements for instance.

"No new opportunities are on the table at this time. Our process will most likely remain as is",
"Acquisition of new business opportunities",
"Increasing regulatory requirements".

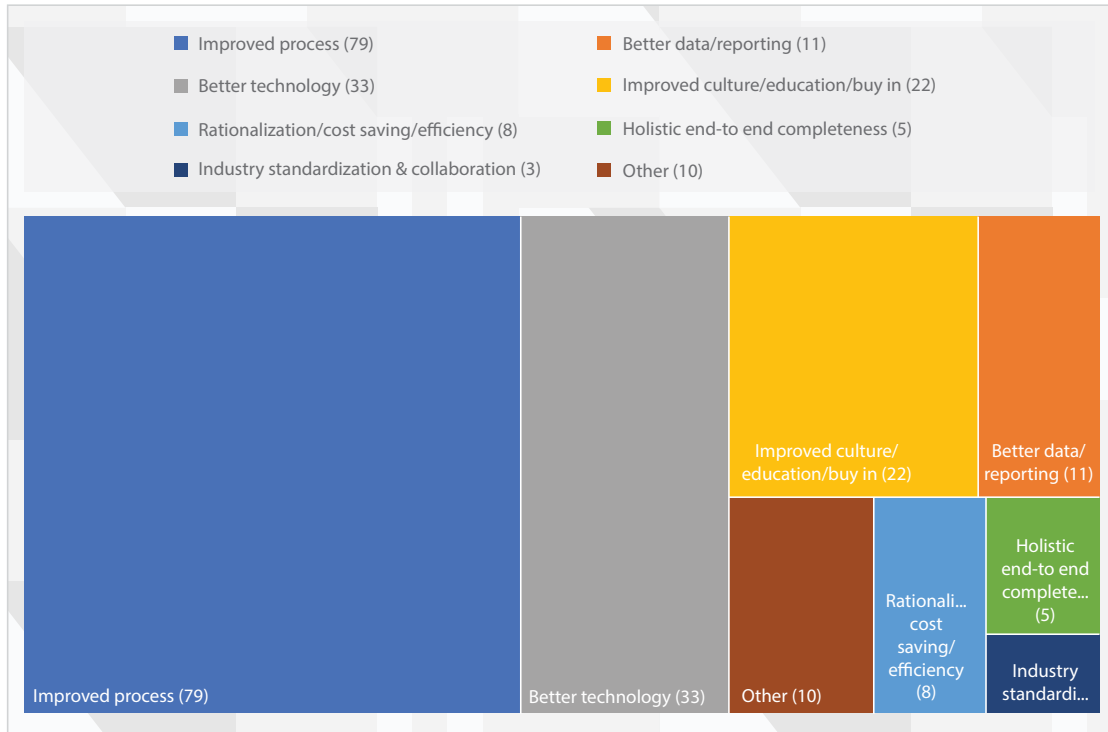


Chart 22: Greatest opportunities for third-party risk management in the 12 months ahead by theme

The Final Word

We also provided participants the opportunity to add anything else they would like to say about their programs.

Responses included:

"Third-party risk is still manual and intensive, with a difficulty to assess the quality of information gathered in assessments and determine if residual risk is within appetite."

Third-party Risk Governance Manager, Bank, AUM > \$100B, UK

"Third-party Risk assessment should cover all suppliers, in all geographies & categories. In fact it should also suggest relevant local or global suppliers to mitigate risks."

Procurement Manager, Technology Sector, Revenue \$5B- \$30B, India

"It's still very difficult to sell the value of the risk management program to a company so focused on revenue generation; important to continue to find ways to balance."

Global Third-Party Risk Manager, Financial Services, AUM \$2B-10B, UK

"Lawyers need to better align contracts for IT security obligations with the IT governance control capabilities underlying the IT solutions provided for complex solutions."

IT Financial Systems Governance Advisor, Asset management, AUM < \$1B, USA

"There is ALWAYS room for improvement."

VP InfoSec Technology Sector, Revenues < \$100M, USA

"Tools and techniques established 50 years ago are not being used today (i.e., decision trees, monte carlo simulation, bow ties)."

Third-party risk analyst, Bank, AUM > \$100B, USA

"It's a challenging and ever-changing industry."

Vendor Program Manager, Bank, AUM \$2B-10B, USA

"Conflict of interest is an ongoing problem for my agency."

Auditor, Government, USA

"Getting executives to truly understand risk"

CISO, Financial Services, AUM \$2B-10B, USA

"To be successful, a top-down Senior Leadership support and enforcement seems necessary."

IT Internal Audit Director, Healthcare Provider, Revenue \$1B – \$4.99B, USA

"Lack of experienced professionals in the field"

Group head of internal audit, Manufacturing, Revenues \$1B – \$4.99B, UAE

"Onboarding; Contract; Ongoing monitoring & reporting of service levels will help to manage Third-party risk."

Risk Manager, Insurance, \$5B- \$30B AUM, UK

"It will be interesting to watch as more and more privacy laws come into play in the US and throughout the globe and how the program has to shift and change to address the regulation compliance."

Data Governance Manager, Asset management, AUM \$10B-25B, USA

"Would like to see regulations kept at a sensible level."

VP/Compliance Officer/Internal Auditor, Bank, AUM < \$1B, USA

"Challenging and dynamic area to navigate."

CEO, Technology Sector, Revenues < \$100M, USA

"Ensure that the internal audit procedures and policies are fully incorporated to assess compliance with corporate risk policies and procedures. This would assist in detecting and managing emerging external threats."

External Sector Officer, Government, Barbados

"Internal efficiency drivers are [a] key driver for Third-party risk management."

Compliance Manager, Technology Sector Revenues \$5B- \$30B, France

"My organization requires lots of training."

Technical Assistant, MIS, Energy & Utilities, Revenues <\$100M, USA

"Ownership of relationship in decentralized and global organizations is challenging, regardless of whether you have a program in place, there is always risk that something could be missed."

Sr. Director, IA, Technology Sector, Revenues \$1B – \$4.99B, USA

"This is a huge topic requiring substantial time and attention, but the journey of 1,000 miles begins with the first steps."

VP, Compliance, Energy & Utilities Industry, Revenues \$5B- \$30B, Canada

"There are still many senior managers / C-suite people in the private company sector that do not understand the "why" on due diligence, as many example cases are focusing on public companies."

Compliance Specialist, Manufacturing, Revenues \$500M- \$999M, USA

"Compliance with regulations is also important given the number of regulations my client has to comply with."

Senior Manager, Professional Services, Revenues <\$100M, USA

"We want to constantly add questions or take them away but the system has limits on when we can do that."

Enterprise Risk and Internal Audit Manager, Bank, AUM \$1B-1.99B, USA

"Concentration risk among cloud providers is a huge concern. - Meeting the increasing demands of the regulators."

Director, Third-Party Risk Program, Bank, AUM \$10B-25B, USA

Methodology & Demographics

Methodology

This survey was conducted during February and April 2020. It was assembled by Aravo Solutions and distributed online by Compliance Week. The objective of the survey is to help organizations benchmark the development of key areas of their TPRM programs.

In total there were 313 respondents to the survey. We removed 36 from the analysis as they had not completed responses beyond demographic details, leaving 277 respondents for the analysis. The survey explored a broad range of issues such as:

- » What levels of maturity are programs at?
- » Do third-party risk programs have the appropriate funding for people, tools and innovation?
- » How are boards of directors engaging with TPRM?
- » What is the typical organizational structure?
- » How are third-party risk professionals remunerated?
- » What are the greatest challenges and opportunities associated with third party risk management?

Quantitative responses are rounded to the nearest whole number. As well as questions designed to provide a quantitative baseline, the survey also asked a number of qualitative, open-ended questions to provide the profession the opportunity to express the challenges and opportunities that they see in their own words.

The survey is intended to be a voice for third-party risk teams – to help the discipline to better understand itself. We hope that it will provide insight into the day-to-day challenges organizations face as they work to get to grips with the rapidly changing landscape of risks and ways of managing them.

What is your level of seniority?

Survey responses came from a range of job levels. Some 33% of respondents are at the senior vice president (SVP), vice president (VP) or director level within their organizations and the C-suite and board of directors represent 6% of responses. Those at the management level represent 39%, and 16% are analysts within the TPRM discipline.

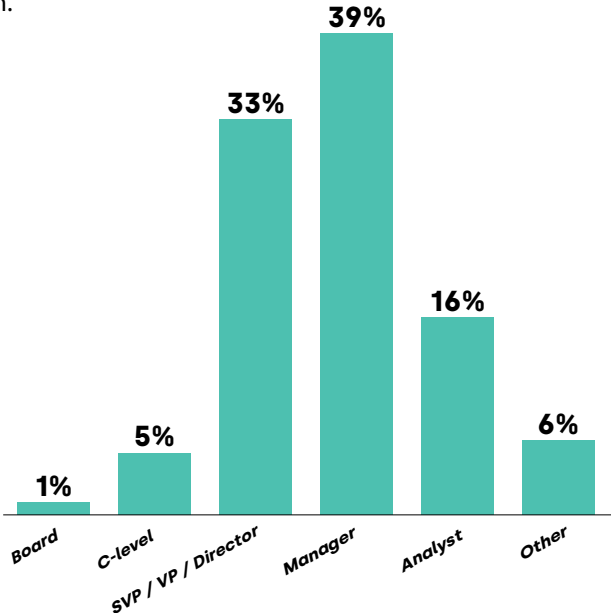


Chart 23: Respondent levels of seniority

Where is your company headquartered?

The survey had responses from around the globe. Some 66% of responses were from US-based companies, with another almost 5% based in Canada.

The United Kingdom was the location for the headquarters of 8%, while the rest of Europe was the home for 7% of organizations.

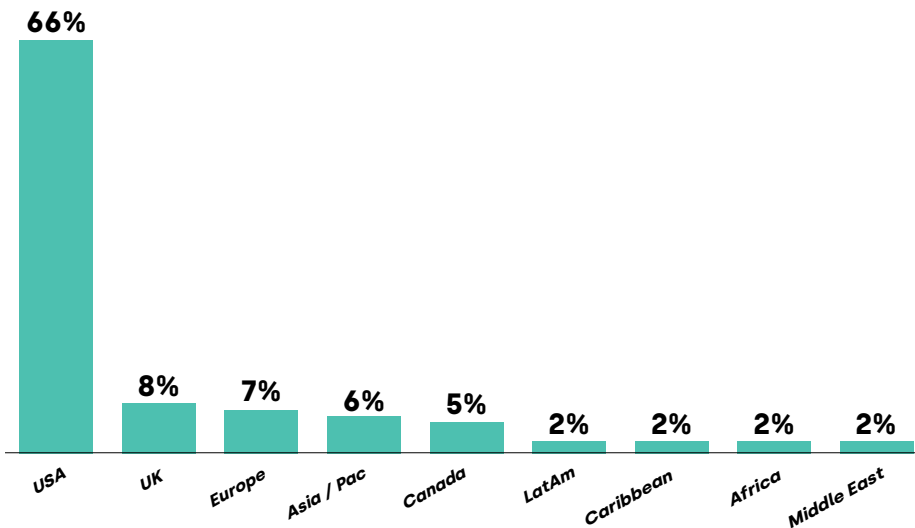


Chart 24: Company headquarters by region

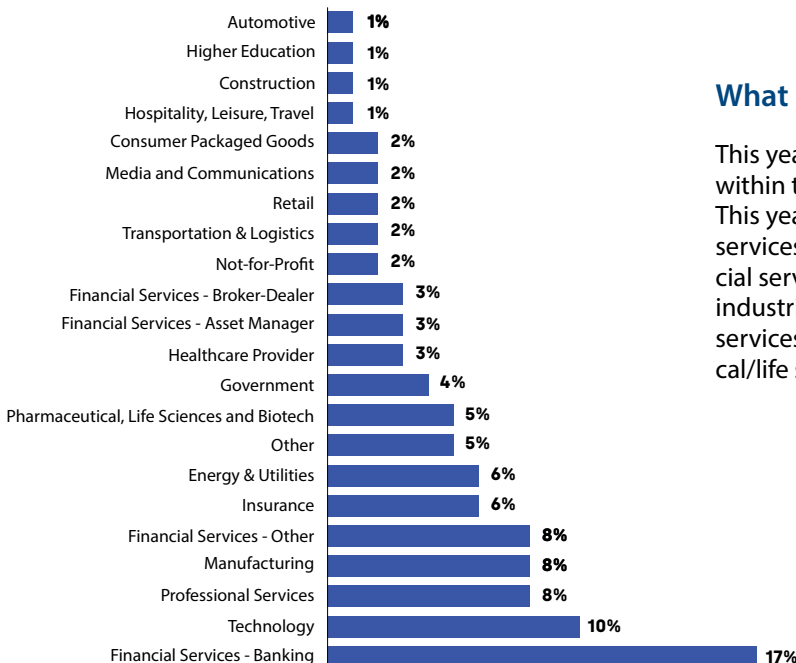


Chart 25: Industries represented in the survey

What best describes your industry?

This year's survey responses were less concentrated within the financial services sector than previous years. This year 36% of respondents were in various financial services sectors, including insurance. The non-financial services respondents came from a wide variety of industries, including technology (10%), professional services (8%), manufacturing (8%), and pharmaceutical/life sciences/biotech (5%).

Size of organization: corporate by global revenue

Overall, the corporate respondents came from organizations of a variety of sizes in terms of global revenue. The largest group (26%) have between \$1 billion and \$4.99 billion in revenues. Some 6% have revenues of greater than \$60 billion, while nearly 19% reported revenues of less than \$100 million.

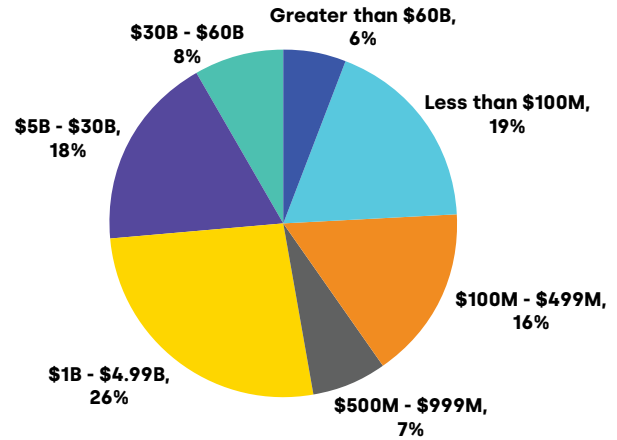


Chart 26: Size of organization: corporate by global revenue (US\$)

Size of organization: financial services – by assets under management (US\$)

Financial services industry respondents came in a range of different sizes. While 18% had more than \$100 billion in assets under management, 20% had less than \$1 billion. Another 34% held assets between \$1 billion and \$10 billion, while 28% were in charge of assets between \$10 billion and \$100 billion.

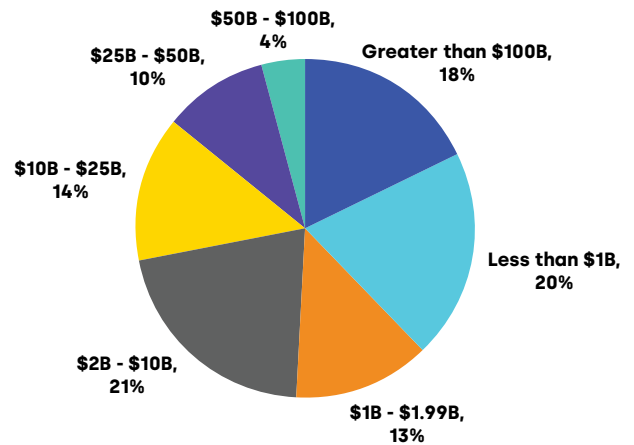


Chart 27: Size of organization: financial services – by assets under management (US\$)

Footnotes

i. U.S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs (updated June 2020), II. Is the Corporation's Compliance Program Adequately Resourced and Empowered to Function Effectively? p.9.

ii. <https://www.ibm.com/security/data-breach>

iii. <http://fcpa.stanford.edu/>