Global CeFPro® Research Report

THIRD PARTY RISK MANAGEMENT

June 2023

CONTENTS

TABLE OF FIGURES

ABOUT US

CENTER FOR FINANCIAL PROFESSIONALS (CeFPro®)

The Center for Financial Professionals (CeFPro) is an international research organization and the focal point for a global community of finance, technology, risk, and compliance professionals from the financial services industry.

CeFPro is driven by high-quality, reliable primary market research. It has developed a comprehensive methodology that incorporates data from its global community and validation by an international team of independent experts.

Examples of some of CeFPro's research include:

- Non-Financial Risk Leaders, the most comprehensive independent study of trends, opportunities, and challenges within non-financial risk.
- Fintech Leaders, an international survey to assess the status of the fintech industry and provide details for informed decisions on technology and business-related matters.
- Third Party Risk Management report is on its 5th issue, providing industry benchmarks on current third-party risks management challenges and opportunities.

To find out more, visit www.cefpro.com/research

ADVISORY BOARD

CeFPro would like to thank the advisory board for the TPRM survey who aided through consultation at each stage of the process. The research originated with a roundtable meeting to determine the survey questions. Following this, each board member participated in the survey and took part in a one-on-one interview to provide context and analysis of the results received.

SURVEY DEMOGRAPHICS AND OBJECTIVES

The Center for Financial Professionals (CeFPro®) conducted a global research study of professionals in the areas of vendor risk, supplier risk, third-party risk, and outsourcing within the financial services sector, including banking. The objective of this research was to provide an industry benchmark of the current status of third-party risk management programs across organizations. It looked to explore governance and team structures to understand where trends and challenges could be identified. This research is the first in an annual series which will review how the industry evolves and the direction of travel for future strategic decisioning.

The global survey ran from 13 March until April 28 and received 212 respondents. Figures 1-3 represent a breakdown of the industry, geography, and regulatory jurisdiction that respondents worked under.

Figure 1: Which of the following best represents the industry your organization is in?

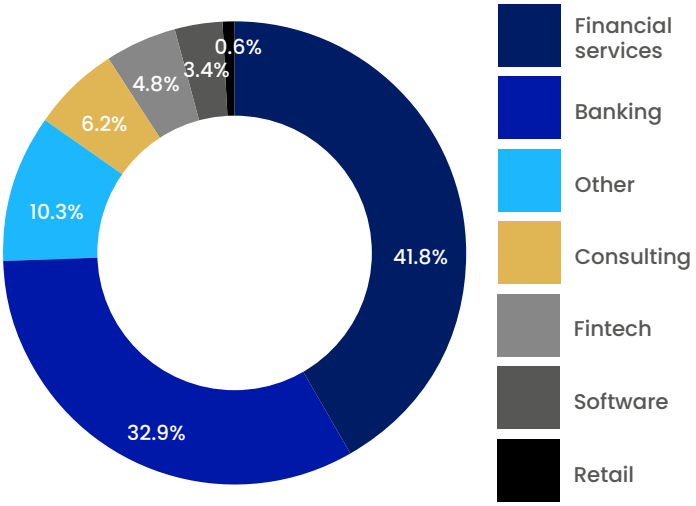


Figure 2: Where are you and your TPRM team located? (please tick all that apply)

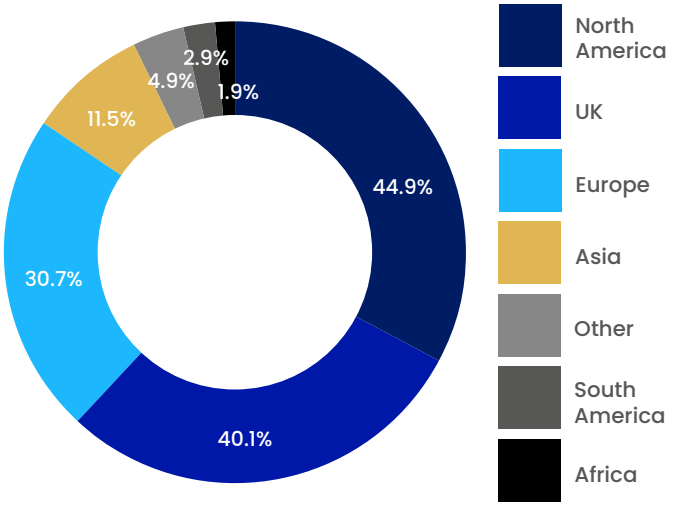


Figure 3: Is your TPRM team compliant to one or multiple regulators globally?

KEY FINDINGS

(Figure 4)

45.6%

45.6% of respondents have a TPRM team of only 1-5 members

(Figure 5)

71.5%

There is no separate oversight committee for intragroup arrangements for 71.5% of survey respondents.

(Figure 6)

78%

Regulatory pressure was viewed as the most important or significant obstacle in managing third-party risk for 2023.

(Figure 7)

50%

50/50 votes towards whether technology developments like ChatGPT and Web3 were important when managing third-party risk in 2023.

The results of the TPRM survey demonstrated disparities across the industry in terms of approach to team structures and management of third-party risks. This report will highlight where the industry has identified consistent trends and where we continue to see a divergence in approaches.

THIRD-PARTY RISK MANAGEMENT SURVEY RESULTS

Third-party risk management (TPRM) continues to gain traction as organizations across industries remain increasingly reliant on outsourced activities and services. In an industry that witnesses continuous digitalization and advancement of product offerings in relation to customer expectations, outsourcing services allows legacy financial organizations to be more agile in their approaches. The Covid-19 pandemic saw a drawback in outsourcing, with many services by necessity being brought back in-house. We are now seeing a trend towards a return to increased outsourcing and reliance on third parties.

As a result, now more than ever effective oversight and understanding of supply chains are critical. Regulators globally appear to acknowledge the risks and are imposing more stringent requirements, with particular focus in some geographies on critical services and looking beyond third parties to understand the risks further than the direct relationship.

STRUCTURE AND GOVERNANCE

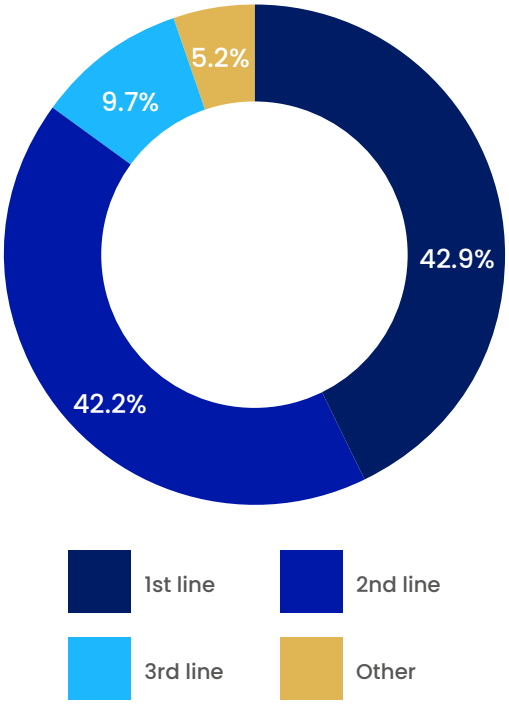
The first area explored within the survey was identifying internal structures and better understanding how organizations manage their teams. 75.8% of respondents stated that their TPRM team sat at a group entity level as opposed to a subsidiary entity level. This demonstrated a more strategic, enterprise view of outsourcing capabilities within many organizations.

A holistic view of outsourced products and services allows for effective insight into the interconnected nature of supply chains and aids in the identification of concentration. Management of third-party risk on a subsidiary level, however, allows for a greater spread of resources across entities. With the increasing complexity and interconnected nature of supply chains, a group level approach appeared preferable.

Within a group or subsidiary TPRM team sit the three lines of defense. The survey explored where TPRM sits within an organization (Figure A). 42.9% of respondents confirmed that their TPRM team sits within the first line, with an almost identical figure of 42.2% stating the second line.

When conducting additional research with CeFPro's TPRM advisory board, it was highlighted that many TPRM teams may sit within a 1.5 or 1B line. While the first line is responsible for day-to-day activities with accountability for vendor relationships, the second line provides the risk function, reporting non-compliance of the first line. TPRM can therefore sit within the first line but hold second line responsibilities. When the team sits between the two lines, it can often have quasi-oversight responsibilities; although not accountable for vendor relationships, it can escalate issues as a true second line function.

Figure A: Does your TPRM team sit within first or second line of defense or in the business?

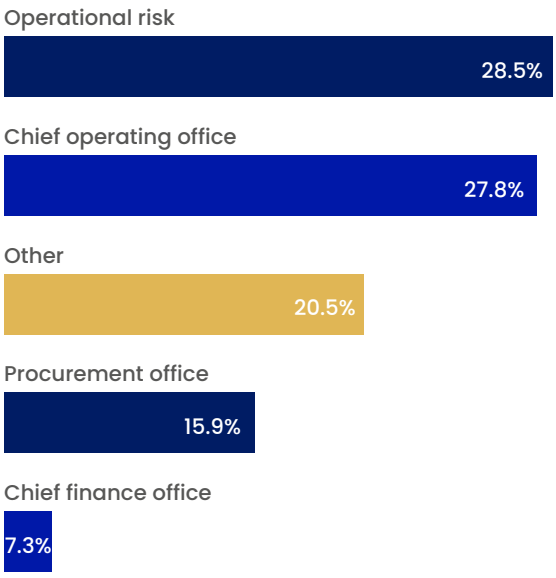


Understanding reporting lines

Further exploring organizational structures, the survey looked to examine reporting lines for TPRM teams. 28.5% of respondents report to operational risk, closely followed by 27.8% that report to the chief operating officer (Figure B). A further 20.5% stated 'other', though no text response was available to provide greater insight via examples of this. Some of the advisory board remarked that this could include compliance or corporate strategy, although this is not the view of the original survey responses.

The other challenge highlighted was that of the reporting chain. For one advisory board member, the TPRM team sits within the procurement office. However, the procurement office sits within the groups chief operating office, so both responses could be representative of their organization. More widely, only 15.9% of respondents stated that their TPRM team sits within procurement, a percentage that proved somewhat surprising to the advisory board members. There was an expectation that more responses would fall within the procurement office to form a holistic first and second line team reviewing the business and risk considerations.

Figure B: What is your reporting line for your TPRM team?



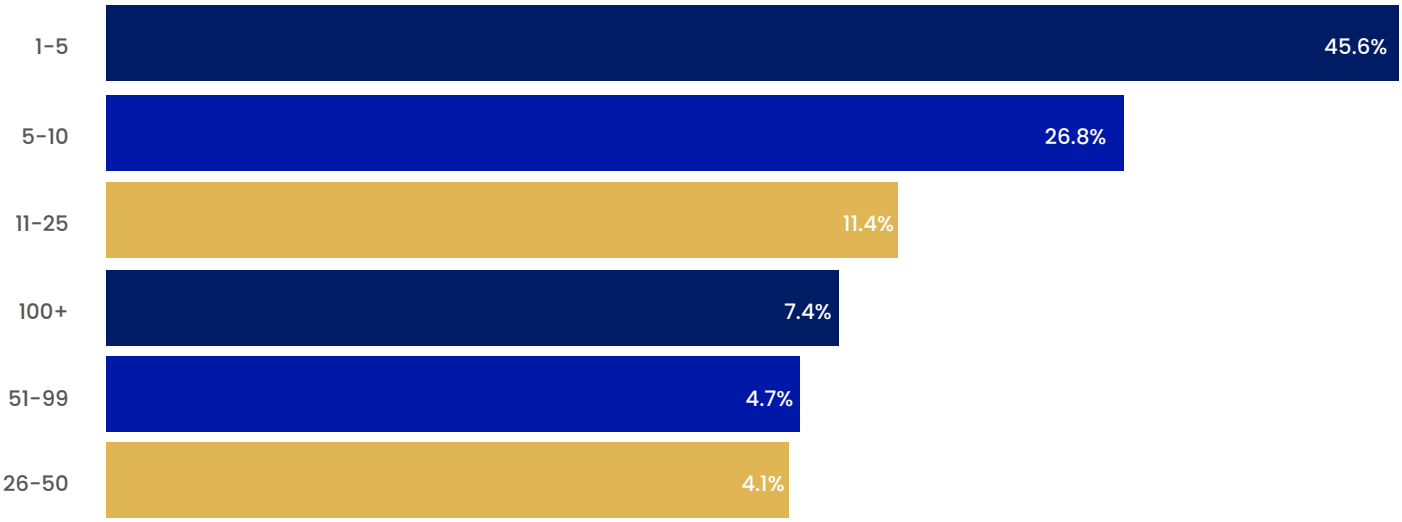
Team sizes

When reviewing the size of TPRM teams, 45.6% of respondents have 1-5 members in their team (Figure B). A further 26.8% have teams of 1-10. These results provoked a mixed response from the advisory board members. Given the 75.8% who mentioned that their team operates on a group entity level, a team of 1-5 appears small for management of group outsourcing. The advisory board offered a range of explanations here, with different-sized organizations reporting different viewpoints. It was mentioned that in some organizations, as seen in Figure B, the TPRM team reports to or sits within the procurement function. Procurement typically forms a much larger team, with risk allocated only a small percentage of resources. This serves to highlight the allocation of resources and prioritization of risk within some organization's TPRM teams.

It was also stipulated that results could be dependent upon within which line of defense the respondent sits; if looking from a business/first line view, teams are typically larger. Within second line functions, teams are often smaller, although there was uncertainty as to the 1.5/1B allocation. Of course, the larger the organization, typically the larger the third-party ecosystem, which would in turn require larger TPRM teams for effective oversight and compliance.

Throughout the Covid-19 pandemic, it was observed that the use of third parties and outsourcing diminished as a result of limited access to services. Maintaining relationships with critical suppliers was therefore prioritized in the face of minimal resources. The industry is now observing a new trend that shows the use of third parties increasing once more as a new normal continues to evolve. As is outlined later on in this report, the third-party risk landscape may have evolved directly as a result of lessons learned and best practices established throughout the pandemic. Third-party risk management has also experienced heightened regulatory focus, with a global influx of requirements to further stabilize the risk. Given the variety of regulators listed in Figure 3, having a team of just 1-5 members managing the volume of third parties and regulatory requirements could highlight the limited value placed on TPRM.

Figure C. How large is your TPRM team?



DEFINING THIRD PARTIES

Across organizations, geographies, and industries, terms within third-party risk management remain interchangeable. The survey explored how organizations are defining third parties and what would fall within the scope of TPRM. The following areas were outlined as falling within the scope of a TPRM team:

- Third parties/vendors
- Intragroup/inter-entity outsourcing
- Non-supplier third parties
- Network providers (i.e., brokers, custodians etc.)
- Financial market infrastructure

While all the above may fall within the scope of third-party risk teams, not all are subjected to the same rigor of testing and oversight. There is an industry shift towards including financial market infrastructure (FMI) under the scope of third-party risk from a regulatory perspective. Given the limited options should an FMI fail, developing an effective business continuity plan is challenging. Therefore, the level of rigor is less stringent, with a view on limiting exposure and risks to service in the case of short-term outage. Resilience regulations indicate that FMIs can be classified as important business services and should therefore fall under the scope of third parties. They may also fall within the scope of critical third parties. However, there is still a lack of industry consensus as to whether FMIs fall within the TPRM scope.

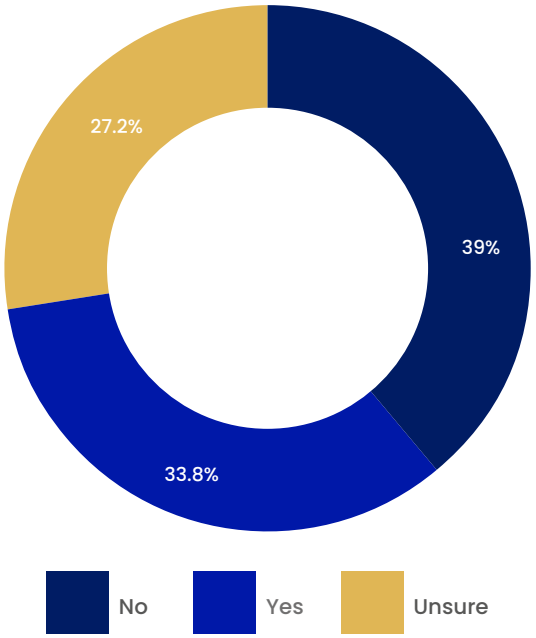
Intragroup arrangements

With intragroup or inter-entity arrangements falling within the scope of third-party risk management, Figure D found that 39% of respondents do not have a separate policy and framework for intragroup arrangements. 33.8% highlighted that they do have a separate arrangement, with a large percentage unsure of their approach. The high percentage of 'unsure' responses, at 27.2%, was alarming.

The advisory board highlighted another trend towards increased intragroup arrangements; with potential uses increasing, teams should be clearer on their organizational structure and whether these agreements fall within their team's purview. For risk professionals, there is an expectation to live and breathe policies and frameworks in order to remain compliant. It was also somewhat surprising to note the almost even split between those who chose yes and no. Given that intragroup and inter-entity agreements fall within TPRM whose teams most often are formed of 1-5 people, it was seen as unlikely that the team could work with two separate policies and frameworks.

When speaking with advisory board members, most had one policy and framework for third parties, irrespective of external or intragroup. They highlighted permitted exemptions and exclusions for intragroup arrangements, but under the same policy and framework. There were also examples of much larger organizations with very different policies and frameworks for intragroup and external arrangements. With internal arrangements having separate challenges including transfer pricing, different background checks and processes are required to manage the different policies. It was also highlighted that the application of policies and frameworks depends on the service provision models. Many firms instruct organizations to service internal and external requirements across entities. This is an example of how industry best practices can differ across organizations and geographies – the alignment, or not, of policies and frameworks can take various forms across organizations and methods of approach.

Figure D. Is your policy and framework for intragroup arrangements separate to external arrangements?



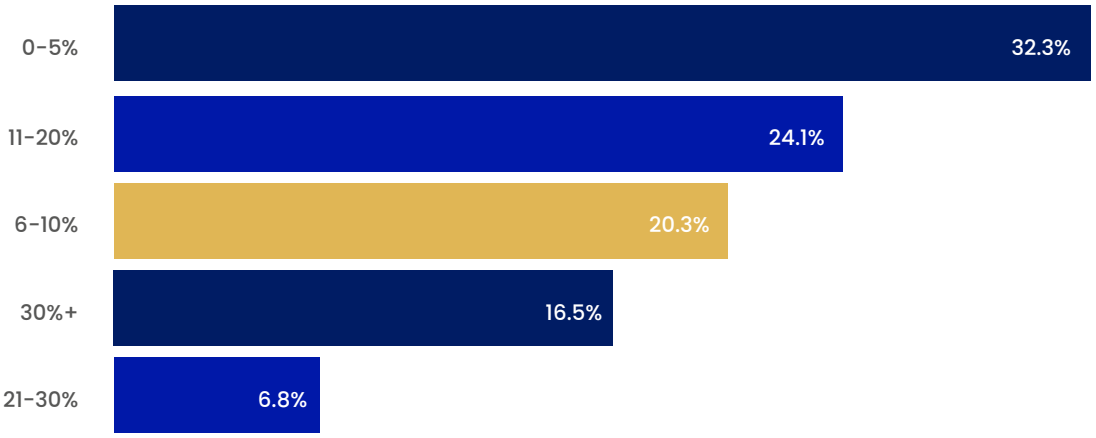
Intragroups: pros and cons

Regulations require organizations to pay particular focus to their critical services and treatment of vendors within intragroup arrangements. 32.3% of respondents stated that just 0-5% of their critical services were intragroup arrangements, with an additional 24.1% citing between 11-20% (Figure E). The results for Figure E demonstrate once more the diversity in approaches, with 20.3% ranging from 6-10%.

Additional research highlighted this diversity, revealing an industry trend towards global organizations leveraging 'hubs' to manage intragroup arrangements; for example, in the area of end-to-end transaction monitoring to limit exposure. This format enables organizations to leverage providers whilst outsourcing internally, providing operational opportunities and management benefits, and better aligning with an organization's strategy. However, as much as intragroup arrangements are subject to the same regulatory requirements and frameworks as an outsourced third party, there are internal challenges and considerations to be aware of, such as potential conflicts of interest and business continuity or exit planning challenges.

With intragroup arrangements posing both pros and cons for organizations, especially when relating to critical services, a range of responses surrounding this approach was not necessarily to be expected. 71.5% of organizations surveyed do not have a separate oversight committee for their intragroup and external (i.e., third party or vendor) arrangements, with 28.5% incorporating a separate oversight committee approach. For those leveraging over 10% of their critical services through intragroup arrangements, it was expected that they would opt for a separate oversight approach. Given the aforementioned regulatory expectations towards intragroup arrangements, as they fall within the scope of the regulatory guidance, a dedicated approach may be valuable to ensure compliance. Intragroup outsourcing is seen as being equally risky as external outsourcing to vendors or third parties. With some advisory board members highlighting a trend towards intragroup arrangements in the wake of the Covid-19 pandemic, could a shift towards their increased use, and the resulting dedicated governance structures, be on the horizon?

Figure E. What percentage of your critical services are intragroup arrangements?

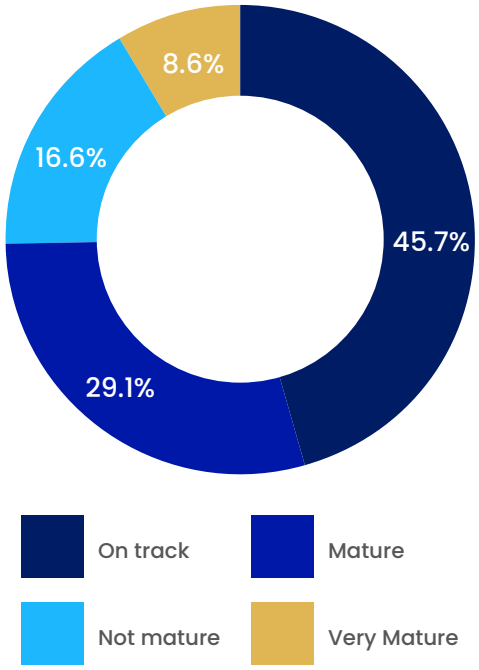


GOVERNANCE

In an effort to understand the maturity of TPRM within the industry to date, as well as where organizations view their progress towards maturity, the survey explored a rating for third-party risk governance and oversight (Figure F). 45.7% of respondents described their program as on track, with an additional 29.1% defining it as mature. These results represent the two middle options, with 16.6% and 8.6% selecting not mature and very mature respectively.

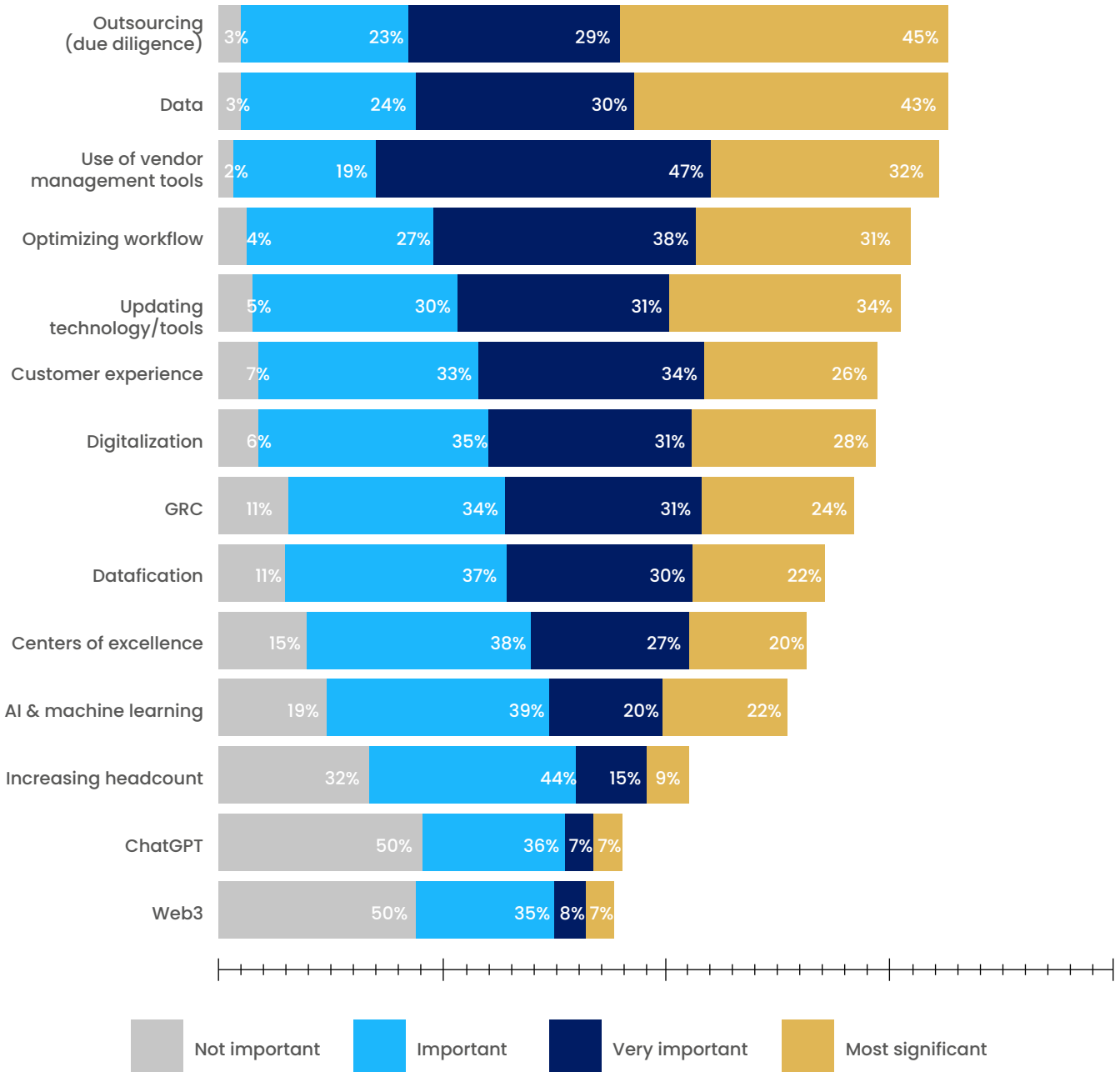
As a discipline, third-party risk management remains an evolving silo of risk management and an evolving discipline in both governance & oversight and regulatory guidance. Therefore, it is unsurprising that fewer respondents scored their programs towards the higher end of the maturity scale. Regulation continues to develop across jurisdictions, with additional requirements anticipated. Much more looks to be on the horizon as a result of the move towards digitization, increased cyber risks, and heightened dependencies on third parties for critical services; all of which have the potential to impact the resilience of an organization. It should also be noted that given resource constraints across teams globally, the introduction of digitization poses an opportunity and a challenge those with resource limitations.

Figure F: How would you rate the maturity of your third party risk governance and oversight?



OPPORTUNITIES

Figure G. What are the biggest opportunities in managing third party risk in financial services in 2023?



The survey then looked to explore the potential TPRM opportunities for the industry throughout 2023. Figure G represents the ranking of these opportunities, with the highest rated area being outsourcing (due diligence). 45% of respondents saw this as the most significant opportunity for 2023, with an additional 29% rating it as very important. This did not surprise the advisory board members, all of whom outlined that they are working towards optimizing programs and advancing their capabilities in order to better manage outsourcing risk and enhance due diligence.

The next most highly ranked area was data, with 43% rating it as most significant and 30% as very important, closely following outsourcing as the front runner. Data sits at the heart of many challenges within third-party risk and better management and interpretation of data present limitless opportunities, including more

effective risk management. When reviewing the range of opportunities listed for 2023, it is clear that many areas rely on data including optimizing workflows, updating technology, customer experience, digitalization, and AI and machine learning. With data as the starting point to success across so many areas, it stands to reason that a key priority for organizations is enhancing data strategies.

The use of vendor management tools also ranked highly as a key opportunity for 2023. The use of vendor management tools also ranked highly as a key opportunity for 2023. Although falling in third with 32% rating as 'Most significant', the additional 40% who chose 'Very important', places vendor management tools in first when combined. This is more aligned with what the advisory board would expect given its signifance across the industry. With so many tools available for standardized rating and due diligence, the opportunities for cost efficiency and enhancing data accuracy are clear. The more opportunities there are to automate these tasks, the greater the opportunity to explore the vendor ecosystem more widely and more deeply to better manage the risk.

Limitations of technology

Technology, however, does not meet the needs of all aspects of a TPRM function. Organizations require the potential for an interim manual solution in order to gain oversight. Often, tools and technologies are built around a specific function, such as procurement, and then incorporated into other areas. This incorporation does not always meet the needs of each group and can result in disjointed systems as the interim solutions are incorporated. While the use of vendor management tools remains a clear opportunity for 2023, implementing a program or group-wide approach tailored to the TPRM function provides a key opportunity in both the near and long term.
Customer experience is another key factor in a successful TPRM program. Assessment of critical third parties should consider support for the delivery of service to customers, not just based on net spend. With third parties relied upon for many customer-facing services, and with the evolution of customer expectations, customer experience should remain a key priority. Disruptions to service, particularly where there is an impact on customers, should therefore be managed as critical.

Falling further down the list is AI and machine learning. Only 22% of respondents viewed this as a most significant opportunity for 2023, although it was highlighted that this is a fast moving area that may gain additional traction within TPRM over the next few years. The same was applicable to ChatGPT and Web3, both of which fell towards the bottom of the rankings. Only 7% rated each area as most significant, with 50% of respondents deeming them as not important. Both technologies are emerging areas with unclear advantages and risks that as yet, are difficult to understand and quantify. Until use cases begin to emerge, it is expected that will they remain lower down the rankings as potential opportunities.

In a fast moving environment, the opportunities for 2023 may be different from those anticipated for 2024. CeFPro aims to track these changes and report their evolution for the next edition of this report.

OBSTACLES

Figure H. Where do you see the biggest obstacles in managing third party risk in financial services in 2023?

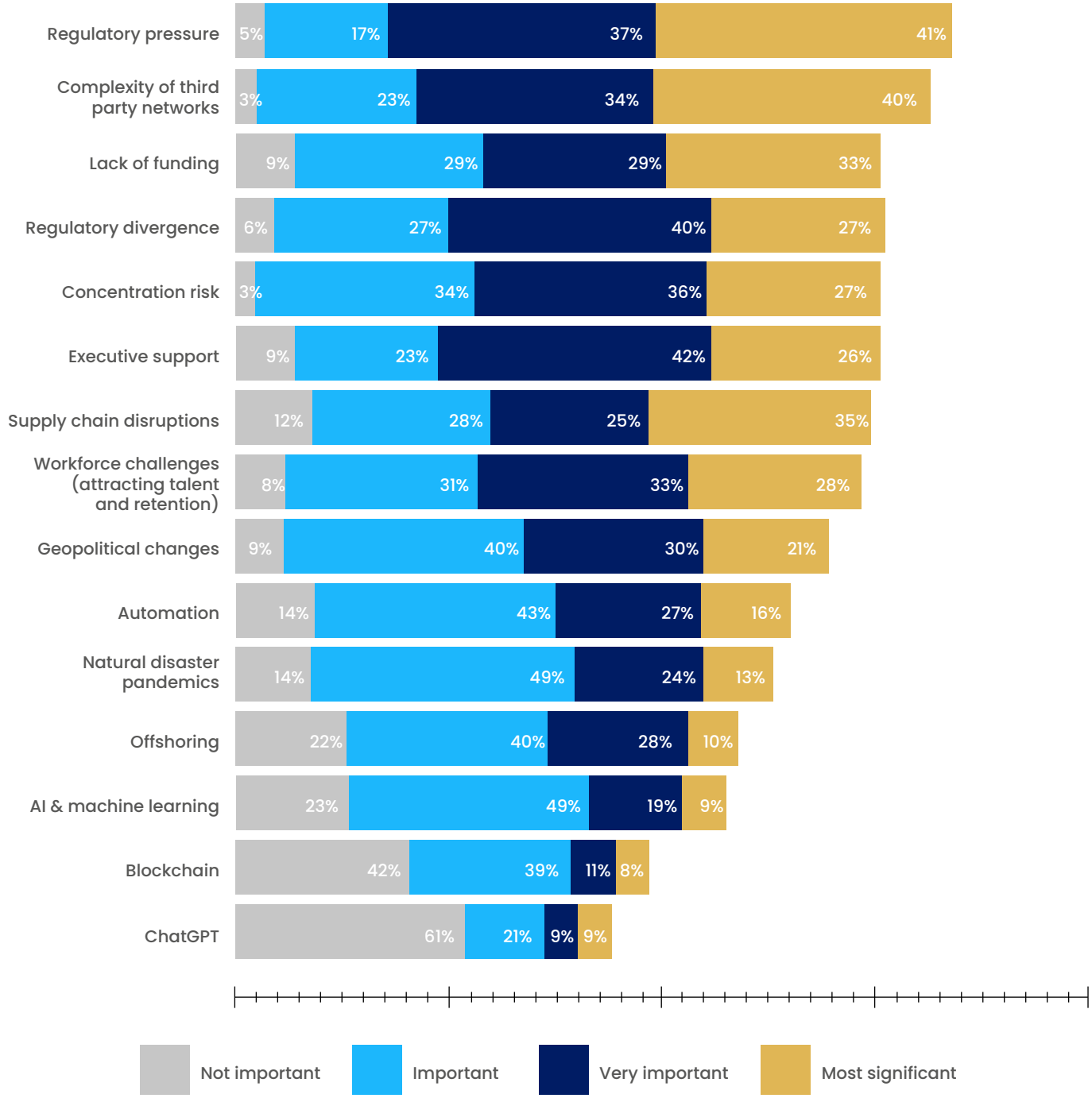


Figure H considers the obstacles ahead for 2023 to help organizations better understand the direction of the industry. Unsurprisingly, the top TPRM obstacle for 2023 within financial services was regulatory pressure – over 40% of respondents rated this as most significant and 37% as very important. As highlighted in Figure F, many respondents viewed their program as mature or on track, with regulation being a main factor hindering the maturity of the discipline.

Just some of the regulatory changes coming into force include the Digital Operational Resilience Act (DORA), with implementation expected in early 2025. Another paper on critical third parties is expected to come through later this year with timelines aligned with DORA, requiring significant work to align the two across European organizations. Another change for European organizations is that of consumer duty, which will incorporate a customer focus. Globally, changes are being introduced across jurisdictions, presenting challenges for those that operate across international borders. Figure B highlights the fact that some organizations are managing this volume of change with just 1-5 team members, it is unsurprising that regulatory pressure is a top concern globally.

Closely related to regulatory pressure is regulatory divergence, bringing two regulatory challenges into the top five. With so many regulatory changes and expectations coming into play over the next few years, challenges remain for global organizations, with 27% deeming it the most significant obstacle and 41% as very important. This surprised some board members representing European organizations but attracted less surprise among those from outside Europe, largely because a trend towards alignment in requirements among European regulators has already been observed. There appears to be a move towards convergence with the UK regulator; for example, exporting its principles for operational resilience and third-party risk management to different countries including Canada, Australia, and Ireland. This convergence means that much can be done to align multiple jurisdictions, with just nuances accounting for the difference. The US is not as aligned, so those board members representing US organizations have not seen the trend towards convergence.

Globally, organizations are calling for better alignment across regulatory bodies, including alignment in terminology and language for definitions such as critical and systemic. Global teams may share suppliers, each with different requirements from their regulators and changing definitions across jurisdictions. This brings challenges for vendors in managing the multitude of requests, as well as for organizations in aligning with the industry and managing operations across jurisdictions.

Managing supply chain complexities

The second largest obstacle for 2023 within financial services is the complexity of third-party networks. As the industry returns to a greater reliance on outsourcing, combined with the aforementioned intragroup and inter-entity arrangements, complexities are continuing to increase. Recent global events including the pandemic and the invasion of Ukraine have highlighted the need for firms to understand the interconnected nature of supply chains. For example, when the Russian invasion of Ukraine began and the resulting sanctions from global economies took effect, visibility was limited on fourth and fifth-party connections. Services had the potential to be disrupted as a result of organizations failing to understand their exposure to Russia and Ukraine across their outsourced activity.

The complexity of networks is not a new challenge – it has always been there. However, regulatory pressures are forcing organizations to become increasingly aware of it. With pressure to extend into the supply chain and legal requirements to understand data transfers with regulations such as GDPR, organizations are now turning their attention to better understanding the interconnectedness of chains.

Third-party risk management is an area with limited funding, as highlighted by the fact that 33% of respondents rated it as most significant and 28% as very important. There is continued pressure and it is often seen as an area lacking investment and support until something goes wrong, such as a vendor incident. Resource limitations may impact a firm's ability for effective assurance and due diligence, including the capacity to manage and oversee intragroup and inter-entity agreements separately.

Further highlighting how quickly the risk landscape can change, areas such as supply chain disruptions, geopolitical changes, and natural disasters/pandemics would have ranked much higher had the survey been conducted 6-12 months previously. With an influx of global events and enhanced risks over the last few years, such as Covid-19, Brexit, Russia's invasion of Ukraine, and continuing global economic challenges, organizations have enhanced their resilience and subsequently view these risks as much lower for 2023. Understanding critical suppliers, fourth and fifth parties, and concentration risks strengthens an organization's ability to manage and weather global events.

Finally, technologies such as ChatGPT, Blockchain, and AI all fell to the bottom of the list as obstacles for 2023. As seen in Figure G, given the relative immaturity and lack of understanding around these technologies, they are seen to present neither a challenge nor an opportunity in the near term.

CRITICAL SUPPLIERS

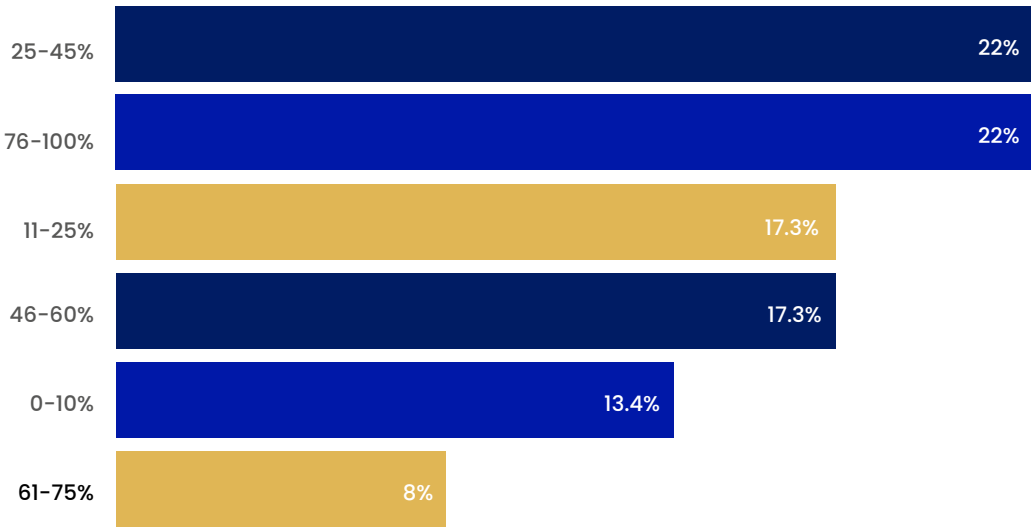
An area which faces challenges around its definition across jurisdictions based on regulatory requirements is that of criticality. Regulators and individual organizations have ranging approaches for defining criticality. The survey explored how many third parties are defined as critical across organizations. The results were divided, with 38.3% claiming 20-100 and 34.8% stating 0-20. The answer is of course representative of the size of the organization and their number of third parties before the critical designation. Therefore, it can be safely assumed that many of the larger organizations would typically have a higher number of suppliers, and thus would also have a higher number of critical suppliers. Without the contextual data, however, this can only be theorized.

Staying with the treatment of critical suppliers, respondents were asked how frequently they conduct third-party risk assessments on critical suppliers as part of their BAU activities. Unsurprisingly, 65.9% fell within the industry expectation of annual assessments, with 13.8% stating an 'as needed' basis, which could require more frequent assessment. The assignment for assessment should be on a risk-based proportionality; segmented based on criticality and level of risk. Given the challenges with resources and funding mentioned earlier within this report, continuous assessment is challenging.

Organizations treat third parties with access to sensitive data to a higher rigor of oversight than those without. For those with access to sensitive data, due diligence and evaluating controls including penetration testing and stock reports are vital. In Figure I, when reviewing the percentage of third parties that organizations conduct due diligence on to evaluate IT security controls and risk management practices, 22% voted 25-45% and another 22% voted 76-100%. This is another example of substantial disparities in approaches across the industry.

Organizations define criticality differently across jurisdictions or companies, so due diligence requirements may differ based on these definitions. As outlined above, some firms only conduct due diligence on those third parties with access to sensitive data, whereas others highlighted a rating scale of 1-4, whereby they decide which third parties to conduct due diligence on based on their level of access and criticality. Some may take a conservative approach and conduct on all levels, whereas others may have the resources to only focus on the highest level.

Figure I. What percentage of third parties does your organization conduct due diligence on to evaluate their IT security controls and risk management practices?



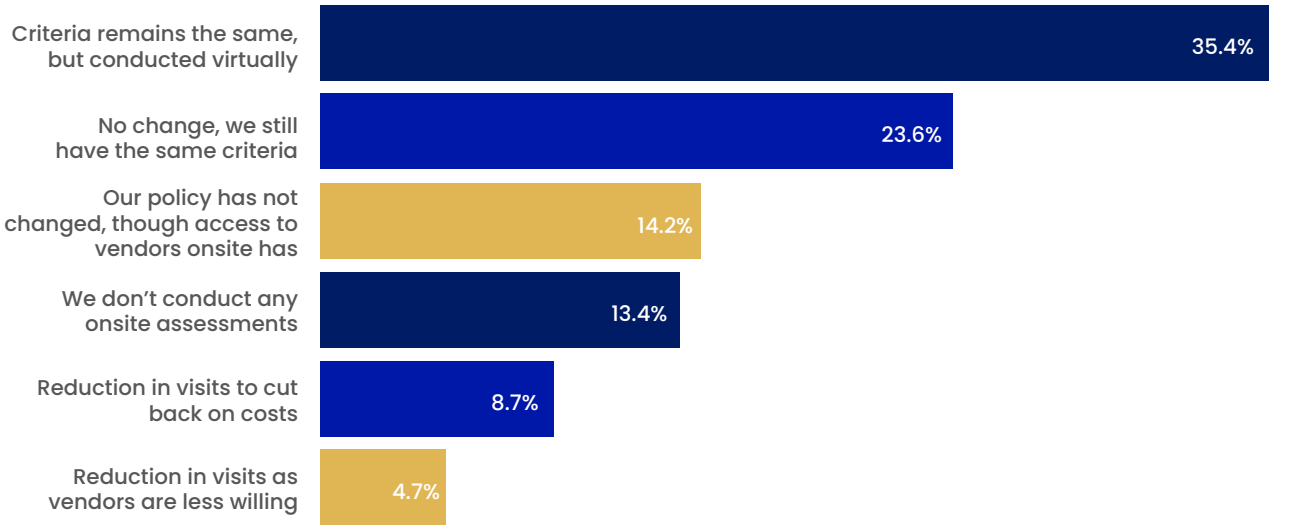
Assessment in a post-pandemic world

Since the onset of the pandemic, typical onsite reviews of third parties have had to evolve. With organizations no longer able to conduct reviews onsite, firms were forced overnight to adopt new approaches in a volatile environment. As a key requirement for critical vendors, and vital to some for effective oversight and due diligence, the transition was challenging. Since the pandemic, however, many firms have continued to operate in an adapted environment, with new approaches and best practice emerging.

The survey explored how these processes have evolved since the pandemic. 35.4% of respondents stated that the criteria have remained the same, but that assessments are now conducted virtually (Figure J). 23.6% reported no change, retaining the same criteria as pre-pandemic. Advisory board members supported these results, outlining the evolution of remote capabilities but emphasizing that there remains a need in some instances for onsite assessments. Many of the requirements for onsite reviews focus on the need for evidence of certain controls and practices. Much of this can be collected virtually, leaving the need for onsite assessments only when physical access is required, i.e., within a data center or to evidence where work is being conducted to assess privacy and security controls.

When conducting onsite reviews from an information security perspective, looking for policies and evidencing ongoing training and penetration testing are key, and some of this can certainly be conducted remotely. As critical suppliers are often technology based, the ability to conduct due diligence and onsite reviews of fourth parties is also often required, adding another layer of complexity. Having the capability to conduct onsite reviews is limited, as is the funding required to put 'boots on the ground'. As regulatory requirements continue to evolve and delve deeper into requirements beyond third parties, adding another layer to review beyond third parties presents an ongoing challenge.

Figure J. How has the process for onsite assessments changed since the onset of the pandemic?



Evaluating concentration risks

Another key consideration for critical third parties is evaluating concentration risks. When asked how organizations primarily assess and manage concentration risk, 43.2% of respondents said they leverage risk assessments and due diligence. However, advisory board members highlighted the need for the industry to set a definition of concentration risk.

Concentration risk can be ascertained by calculating the percentage of work outsourced to a singular vendor, or the percentage of an organization's work in relation to the third party's overall portfolio. If organizations outsource a large amount of their work to a single vendor, they expose themselves to concentration risks. Having the capability to conduct business continuity plans and stressed exit plans on a third party responsible for a high volume of tasks is challenging. The second definition relates to the health of the third party, and the proportion of their work carried out for any one organization. If the third party is smaller and a single organization forms a large percentage of its portfolio, the financial health and viability of that third party could be questioned. Reviewing the size of third parties in this scenario is key to ensure they are financially viable and secure.

Organizations have been impacted by concentration risks and are therefore increasingly conscious of the impacts. Identifying concentration, understanding its impact, and managing it all form key aspects of a TPRM program. Organizations need to review alternative vendors and plans, and look towards ways of limiting or segregating the risk.

CLOUD

Closely aligned with the increased risk of concentration comes the consideration of cloud service providers. As the industry moves towards reliance on cloud services, organizations place a huge amount of trust in a limited number of third-party providers. With access and responsibility for storing vast amounts of sensitive data, cloud providers have the potential to cause huge disruption. A limited number of providers have monpolized the industry, having an impact on organizations working with them. As an organization in high demand, with limited cometition, third party risk oversight and assessment remains challenging. Some larger organizations remain reluctant to allow for detailed due diligence or onsite assessments. The limited opportunities also pose a concentration risk across financial services, with so many reliant on so few service providers.

The survey looked to explore approaches to managing cloud risk. 47.7% of respondents stated that they did not have a unique process specifically targeted to managing cloud risks when conducting due diligence. 27.7% did have a unique process – of these, some examples included:

- Automated and manual controls and logging OS inventory
- CASQ industry assessment
- Cloud computing questionnaire
- Risk and contractual clauses
- Specific security controls from what would be applied to a non-cloud service provider
- Greater involvement from infosec and operational resilience
- Hosting review board process
- Internal GRC committee
- Onsite assessment for cloud provider
- Reviews performed by multiple departments to assess the impact
- Separate review by specialist infosec team for critical cloud suppliers, in addition to the normal due diligence process; shared control responsibilities definition
- TPRM policy statement
- Technology escrow agreements

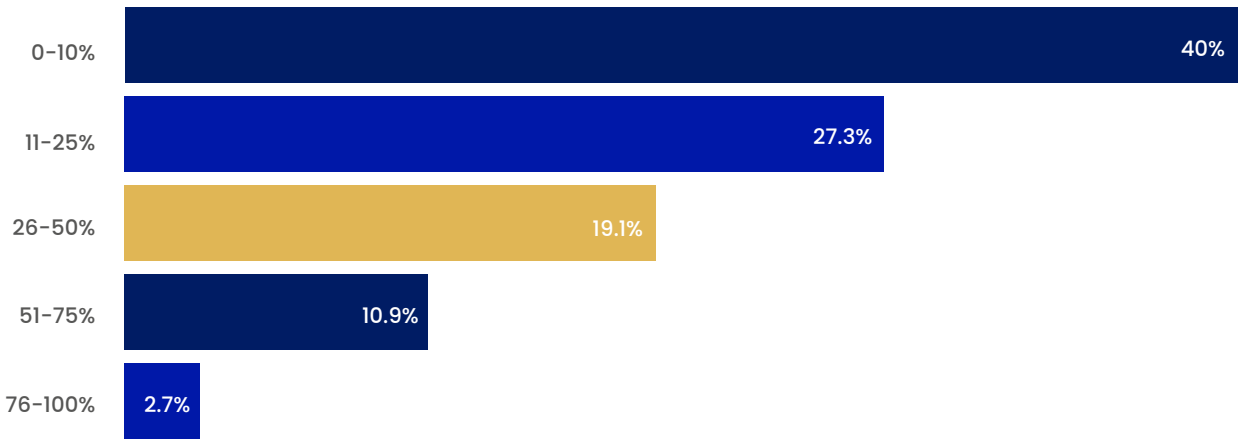
BCM & INCIDENT RESPONSE

Business continuity and incident response plans increasingly play a key role in managing third-party risks. The survey explored the percentage of incidents caused by third parties over the last five years (Figure k). 40% of respondents estimated that 0-10% of incidents were caused by third parties; 27.3% selected 11-25%; and 19.1% reported 26-50%. However, not all respondents would be privvy to a broader view of their organizations events and therefore answers could vary when conducting outside of third party risk.

With many only able to identify incidents occurring as a result of third parties, the broader scale of incidents outside of TPRM could vary. The definition of an 'incident' may also vary across organizations. Some may view any disruption of service, no matter how minimal or brief, as an incident, while others may have criteria in place regarding the length of time the disruption lasted, or the impact to customers. Work on root cause should therefore be conducted to increase accuracy of the designation of a third-party related incident.

Often there is a knee-jerk reaction to blame a third party and mitigate the reputational risk. However, internal challenges may in fact be the root cause – an internal change could have an impact on the third party, which then leads to an incident. This would quickly be designated a third-party incident, yet the origination lies with the organization that made the initial change. Conducting root cause analysis will enable organizations to better understand their position and determine whether an incident is truly a third-party risk or as a result of challenges with internal controls or changes.

Figure K. Over the last 5 years, what percentage of incidents have been caused by third parties?



Respondents were prompted to leave a text response when reviewing how their organization assesses the impact of a vendor-related data breach on the business, including financial and reputational impacts. Figure L represents some of the key responses:

Figure L. Text comments on how organizations assess the imapct of a vendor related data breach

"Assessments are performed by compliance, information security, and privacy specialists as part of vendor approval. Risk level is assigned based on likelihood and impact, which govern the controls that will be required to mitigate risk based on cost, reputation, and impact to clients."

"Events such as breaches are reporting in a risk/GRC tool, where assessment of impact is performed by the business owner and reviewed and challenged by 2LoD."

"Lost revenue, reduced market share, reduced market capitalization, secondary losses, e.g., fines, penalties from regulators."

"We measure the number of stories in the news about any data breaches relating to us or our vendors."

"We have an incident response team who is engaged and will opine with legal and regulatory compliance to determine severity of the breach, whether regulatory GSE and client notifications must be sent and credit monitoring to customers impacted. We would also review the vendor's handling of the incident, their transparency in root cause, and remediation to determine if they need to be replaced."

"We have a privacy and cyber team who will assess and determine impact and engage stakeholders from compliance, legal, and client management as well as vendor owners, to determine the severity and appropriate cause of action to handle through remediation."

"Deep look at the size, scope, and complexity of each situation/ event/incident."

"Fully document the entire interconnected nature of our supply chain but we focus mainly on the mitigation or the ramifications of these impacts via technology escrow agreements."

In order to produce and execute effective business continuity and incident response plans, organizations need to ensure they understand the risks and monitor the full third-party profile. One approach outlined in Figure J was monitoring news stories. Looking at social media and the use of unstructured data to better inform judgement on the status of third parties is increasingly being leveraged. If a contractor or subcontractor has an acceptable social media presence, it can be an indicator of security or risk. Softer checks by reviewing outlets such as LinkedIn, Twitter, news websites, and business bureaus can provide an insight, especially when the third party has access to data. Other forms include leveraging state, federal, and local social media sites to ensure there is no negative news or publicity. ChatGPT is an emerging area that could be used to scan the internet for such reviews and glean a positive or negative response.

CONCLUSION

The future of third-party risk management is fast evolving, and the next few years hold countless opportunities for growth as well as disruption. There remain some key obstacles on the horizon, such as the threat to information security/cyber risk exposure from increasingly complex supply chains. As TPRM teams continue to advance their technical knowledge and become sharper in their understanding, so do bad and threat actors, with techniques including phishing, ransomware, and the use of the dark web continuing to evolve at a rapid pace.

The financial and reputational risks associated with third parties also continue to develop. The risks of financial losses as a result of a third-party service disruption remain unquantified, while the potential reputational damage to an organization from a third-party outage also has untold repercussions.

In an increasingly online and digital environment where news travels fast, organizations face a new risk. As was seen with the 2023 Silicon Valley Bank collapse, initial news stories sent shockwaves across the industry and helped drive the run on the bank. The events of the last few months have shaken consumer confidence, so organizations must continue to hold third parties to the highest level of scrutiny, oversight, and due diligence in order to restore confidence and ensure security.

OTHER CEFPRO REPORTS

Center for Financial Professionals offer an extensive library of market intelligence reports available to download for free with CeFPro Connect:

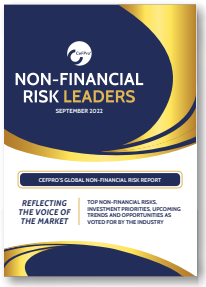
FINTECH LEADERS 2022

Find out just how much the the rapidly evolving financial technology industry is changing year on year by reading the Fintech Leaders 2022 report. With the outcomes of the 2023 results in mind, how has the landscape changed in just one short year since we last heard from the industry experts that are involved with fintech day in, day out? Whilst this year's research was conducted during a time of global sanctions and economic volatility, the 2022 report came around at a time when the world was adapting to a new normal as we emerged from the Covid-19 pandemic. Was the industry's reaction to the pandemic the same as that of this year's events? Are there any differences in what was deemed an opportunity? Have investment priorities changed in such a short span of time? Download the Fintech Leaders 2022 report to gain a complete understanding of the financial technology industry and how external events are having an impact, enabling you to full understand how the industry is changing and successfully plan the future ahead.

ESG STATE OF PLAY: BANKS COMPLIANCE AND AUTOMATED REPORTING TRENDS

Conducted in partnership with solution provider Workiva, ESG state of play seeks to establish where the industry stands with ESG reporting, and benchmarking technology capabilities with the influx of ESG changes that are occurring as ESG continues to gain prominence within the industry. This report centers around expectations for increased regulatory change and scrutiny as banks increasingly incorporate ESG mandates within their operations.

NON-FINANCIAL RISK LEADERS 2022 REPORT



Non-Financial Risk Leaders is an annual report providing clarity on upcoming trends and opportunities within non-financial risk, including a top 10 ranking of the most prominent non-financial/operational risks as voted for by almost 1000 industry professionals. With non-financial risk rapidly building momentum and encompassing some of the most volatile risks of current times, the ability to understand the cause and effects of these risks and how to overcome them is essential for any institution looking to rise above the rest and prepare for their future. Non-Financial Risk Leaders is your new go-to resource for doing so.

EFFECTIVE SPREADSHEET MANAGEMENT

Conducted in partnership with Incisive Software, this report investigated the current industry status of management and oversight of spreadsheets, and what methods institutions are using to establish solid foundations to promote accurate date used to support critical business decisions. The findings of the survey aim to provide insight into the key benefits companies can expect to receive from an effective spreadsheet management program.