Center for Financial Professionals

Supported by ARAVO

THIRD PARTY RISK: A JOURNEY TOWARDS MATURITY

Results of the 2018 'Taking the Pulse of Third Party Risk Management' Survey

May 2018

WHO WE ARE

Aravo Solutions delivers award-winning, market-leading cloud-based solutions for managing third party governance, risk, compliance and performance. We help companies protect their business value and reputation by managing the risks associated with third parties and suppliers, and to build business value by ensuring that their third party relationships are optimized.

Aravo TPRM for Financial Services allows firms to centralize all their third parties into a single, quick-start cloud solution for assessing risk, conducting initial and ongoing due-diligence, managing and monitoring contractual compliance and performance, and transitioning and off-boarding third parties.

Providing unrivaled regulatory agility and ease-of-use, together with actionable executive reporting, Aravo supports a user base of 136,000 corporate users, managing more than 4.5 million third party users in 36 languages and 154 countries.

Learn more at aravo.com

Center for Financial Professionals

The Center for Financial Professionals (CeFPro) is an international research organization and the focal point for financial risk professionals to advance through renowned thought-leadership, unparalleled networking, industry solutions and lead generation. CeFPro is driven by and dedicated to high quality and reliable primary market research; helping us provide our audience with invaluable peer-to-peer conferences such as our flagship Risk EMEA and Risk Americas series.

CeFPro also boasts knowledge sharing platforms, such as: Risk Webinars, Research Reports and Risk Insights. Risk Insights is written by the industry for the industry and now covers online articles, a quarterly Risk Insights Magazine and Risk Insights TV.

Learn more at www.cefpro.com and www.risk-insights.com

TABLE OF CONTENTS

INTRODUCTION AND METHODOLOGY

Third party risk management (TPRM) is in the relatively early stages of its journey of development as a discipline.

What best practice is, how regulators around the globe are approaching TPRM, and in which ways TPRM intersects with various teams across an organization, are questions to which the answers are continuing to evolve. TPRM teams are challenged with putting in place a robust management framework and meeting compliance targets while the world around them morphs at stunning speed—regulations, the business environment, the digital environment and risks.

METHODOLOGY

The research for this new survey was conducted during March and April 2018 and was put together by Aravo Solutions and distributed online by the Center for Financial Professionals, an impartial and independent financial research and event organizer. The objective of the survey was to help organizations benchmark some of the key areas of their TPRM programs. There were 211 respondents to the survey, which explored a broad range of issues such as:

- Levels of program maturity.
- Whether third party risk programs have the appropriate funding for people, tools and innovation.
- 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?

The survey is intended to be a voice for practitioners, providing insight into the practical reality and challenges facing third party risk teams in this rapidly evolving discipline.It should be noted that the majority (79%) of respondents were from the financial services and insurance industries, so results are more representative for these organizations.

The Center for Financial Professionals provided the raw data findings, correlations and a basic analysis of the data to Aravo Solutions, who provided the final analysis and interpretation for reporting purposes.

We would like to extend our sincere thanks to all those that participated. The findings are intended to help firms develop their road-map to maturity, and help with planning, resourcing and direction.

The results show that TPRM teams recognize that they face significant implementation challenges, and that they worry about their ability to keep up with the velocity of change.

Yet, they are also optimistic about their ability to deliver true value to the business as they build out their TPRM programs – through having a golden source of data, improved analytics, and better reporting about their third parties.

KEY FINDINGS

The survey results provide a very interesting snapshot of a discipline in development – one that is still in its formative period, but with its sights set high. Key findings include:

- Most organizations are at a relatively early stage of their TPRM journey – two-thirds of respondents report their programs were developing, defined, or in the initial stages of maturity. Many organizations lack dedicated resources or have only small teams, for what is becoming an increasingly complex, dynamic and scrutinized function.
- However, nine out of ten respondents expect their budget to either grow or stay the same over the coming 12 months, signaling that most organizations – in these times of tight margins – are serious about developing and maturing their TPRM programs.
- While regulatory compliance is the primary key driver for nearly half of organizations, business and cost benefits were primary drivers for more than four out of ten respondents.
- Organizations are gravitating toward locating their TPRM function within the risk management team, and are using a centralized structure that aligns to the organization's overall approach to risk management. Examples of this include the use of risk assessments and development of a risk appetite. On average, programs are actively managing nine distinct risk types.
- Organizations are still struggling with some of the basic components of the TPRM lifecycle, such as capturing all third parties in a single inventory, conducting due diligence, and reporting. Many of these challenges are due to a lack of technology investment – two-thirds are using spreadsheets for at least part of their TPRM program. Some 44% are using Sharepoint.

Two thirds of respondents indicated that their TPRM programs were in the earlier stages of maturity: initial, developing or defined.

91% of budgets to remain the same or grow in the next 12 months

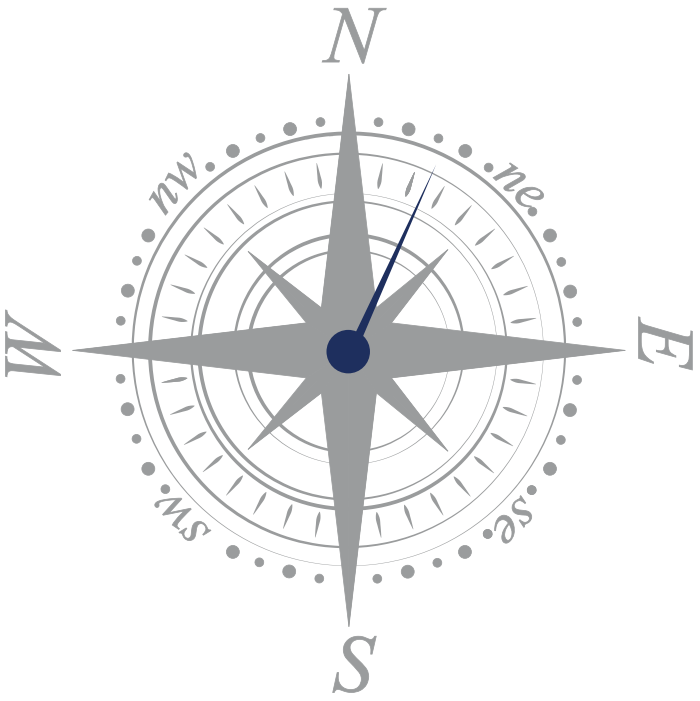
Regulatory compliance (49%) and business-associated benefits (41%) were the primary drivers of TPRM programs

83% of respondents currently have, or are gravitating towards, a centralized model of third party risk management

Creating a single inventory; implementing due diligence coverage; fast and accurate reporting; and technology restrictions are among the biggest hurdles respondents face in their journey towards program optimization today.

KEY FINDINGS

- TPRM teams are concerned about being able to keep up – with regulatory change, with the growing demands of an extended enterprise, and with the evolving nature of risk.
- This last point includes such hot button topics as cyber risk, data security, and concentration risk. While respondents were excited about the ability of TPRM to deliver real business value, they also recognize the importance of having the right infrastructure in place to support their TPRM program.
- Overall, it seems that respondents are very aware of how TPRM can help their organizations – well beyond pure regulatory compliance – but sense that they will need to evolve their programs quickly to stay ahead of the very risks they are trying to mitigate.
- Of all of the shortcomings of the current state of TPRM implementation, it is perhaps reporting that should cause the most concern. After all, it is through good reporting that TPRM will be able to communicate its value to key stakeholders such as senior management, the board, and regulators. Capturing the right information is the first challenge for firms – but being able to extract that information quickly and easily for analysis and decision-making is perhaps a bigger, second challenge. This is fundamental - not only will boards require accessible reporting for good governance, the lack of ability to quickly and comprehensively report will be a red flag to regulators.



Reporting is a key challenge for TPRM, with the majority of respondents unable to deliver standard reports quickly and completely.

Challenges

"Development of [a] system that has the flexibility to manage the ever-evolving requirements (regulators, markets, products) that we face when managing our vendors."

Enhanced Due Diligence Manager, asset management firm, greater than $100B assets under management, UK.

"Identifying and managing risk associated with new technologies, and balancing risk versus the need or demand for those new technologies."

IT Specialist/Vendor Management Specialist, bank, $1B-1.99B assets under management, USA.

Opportunities

"Showcase the true value from a vendor assurance program that is risk-driven and enables the business to see the value added."

Manager - Vendor Security Assurance, corporate, $5B-30B revenues, Netherlands.

"Technology is changing quickly and analytics capabilities using machine learning are reducing manual efforts and providing better information faster."

Sr. Director, bank, greater than $100B assets under management, Canada.

PART 1: MATURITY & DRIVERS

This section of the survey explores how organizations self-identified their relative levels of TPRM program maturity.

TPRM goes through stages that reflect the maturity of its framework, people and processes - starting with initial, and then moving through developing, defined, established and optimized. The survey sought to capture perceived maturity level and, where relevant, correlate it against other responses in the survey.

In addition to maturity, it looks at what the key driver behind each respondent's TPRM program currently is.

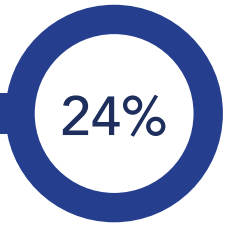
Which maturity level do you consider most closely describes your overall third party risk management program?

OPTIMIZED

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 three Lines of Defence. 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.

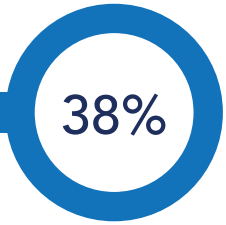
ESTABLISHED

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.



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.



DEVELOPING

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.

INITIAL

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.

OBSERVATIONS

The spread of maturity levels within the pool of respondents reflects the evolving nature of third party risk management. Just 28% of respondents said their organization had an established program, while only 5% claimed to have an optimized one.

This leaves much room for evolution and growth. Most respondents – 38% - said their programs were developing, while another 24% indicated that they were defined. Some 5% said their organizations were in the initial stages of creating a TPRM program.

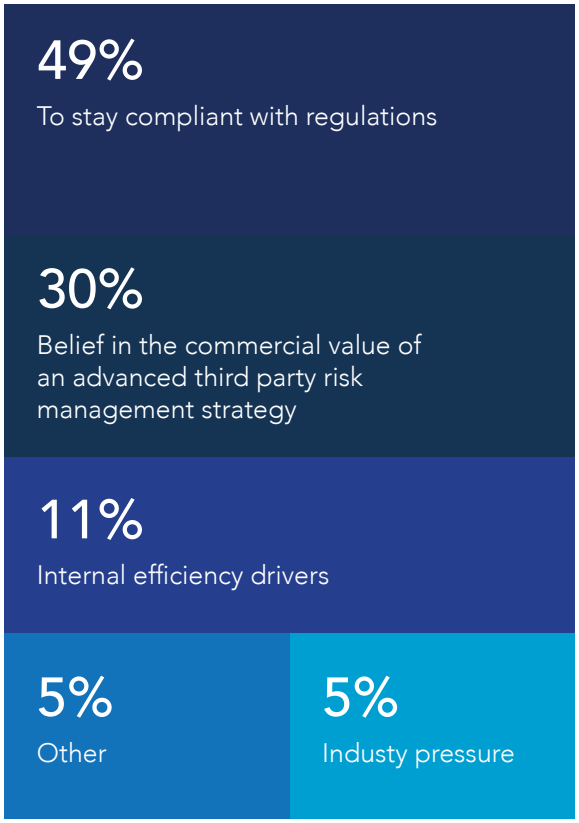
Regulatory pressures on financial services organizations to develop explicit TPRM programs are likely to accelerate development over the next few years in that sector. In other sectors, concerns over issues such as cyber risk, information security, and data privacy within third party relationships could potentially contribute to a more urgent emphasis on strengthening programs and working towards advancing maturity.

What is the primary key driver for third party risk management in your organization?

Nearly half of organizations said the primary driver for the development of their TPRM programs was staying compliant with regulations. In the current environment, this is not surprising. In the US, banking regulators have updated their approach to TPRM program examination over the past 18 months, and this year, 2018, in the UK, the FCA will be assessing the risks of outsourcing and third party providers in firms during several thematic reviews, with the aim of understanding not only how financial services organizations are using outsourcing providers, but also how use of those providers may create potential concentration risk within the sector.

Other regulatory efforts – such as the introduction of the General Data Protection Regulation (GDPR) in the EU, as well as increased government and supervisory focus on cyber risk and data security within third party relationships – are also turning up the heat on firms' approach to managing these partnerships.

However, it's not just the 'stick' that is the motivational force behind programs - it is also the 'carrot'. Of the respondents, 30% are putting their TPRM programs in place because they believe in the commercial value of having an advanced TPRM strategy. Indeed, many argue that TPRM is about far more than just regulatory compliance, and that it can contribute to delivering a competitive edge for organizations through richer, deeper, and more transparent relationships with vendors and partners.



Another 11% of organizations cite internal efficiency drivers as their primary key driver – showing another way in which TPRM can deliver value. Internally, coordinating and streamlining third party risk management can remove manual and duplicative processes across an organization. Program maturation and development was seen by many as a key opportunity by many to improve operations and outcomes.

Just 5% indicated industry pressure to adopt TPRM practices was a driver – however, it's possible this could increase over time, as TPRM programs begin to ask for information about fourth party relationships, and there is additional pressure to raise the 'collective bar' of security and safety across entire ecosystems. Already, some ratings companies are recommending negative votes for boards or board members based on poor cybersecurity risk ratings, for instance.

Of those who selected "other", the most often cited primary driver was risk management. Says one respondent, the "goal is to manage risks", while another cites the "fear of breach of law and regulatory requirements and not knowing the full risk landscape beyond the 'critical' outsourcing relationships". A third said that the organization wanted to 'understand and mitigate the risk to our operations'. However, one respondent also spoke of the contribution that TPRM could make to the future of the organization, saying that their primary driver was 'innovation/product development.'

OBSERVATIONS

These two questions provide some key insights into the state of third party risk management at organizations today, including:

- It's still early days for the development of TPRM programs at most organizations. Two-thirds of programs are either in the initial, developing, or defined stages.
- Regulatory compliance is a very important driver of TPRM program creation and development. Given the concerns that governments and regulators have around key TPRM issues, such as cyber risk, information security and data privacy, it's likely that pressure on TPRM framework development from those quarters will continue for some time.
- There is, however, a substantial minority of organizations who recognize the potential business benefits that the TPRM discipline can bring. Organizations which are in the early stages of TPRM development should be sure that the framework they put in place is open to exploiting these potential business benefits.
- Part of the challenge with driving maturity is both the complexity and pace of change associated with third party risk – which makes it an ongoing game of 'catch-up'.

"Increased social perception and expectation of organizational responsibility is driving many of the required changes (including regulation). However, the increasing complexity and dynamism of supply changes and technology is currently creating significant challenges."

Resilience manager, asset management firm, greater than $100B in assets under management, UK.

PART 2: THIRD PARTY RISK ORGANIZATIONAL STRUCTURE, RESOURCE AND BUDGET

Third party risk management is a relatively young and evolving discipline, and as such, organizations are often looking to understand how others are approaching it. One of the objectives of this survey was to understand the operational management of TPRM and the approaches of those organizations that rate their programs as more mature (established and optimized) were taking.

A hallmark of third party risk programs is the number of stakeholders involved in its management and success. Regulators have made it clear that they expect Board and senior management governance and oversight. Across the organization many play a role too: LOB relationship owners, procurement, risk, compliance, IT, legal, and finance – all contribute to elements of a program. However – who owns it? Depending on industry, on culture and on what may be immediate risk priorities of an organization, TPRM can be located under different functional areas.

In addition to the question of where TPRM is located, there can be very different models of management and governance. Immature disciplines are often managed in a more ad-hoc and decentralized way as they emerge due to specific, immediate needs (such as information security) and are disconnected from a single view of enterprise vendor risk. As they evolve and mature, standardized processes emerge, and management can gravitate to a more centralized approach. Where does third party risk sit in this spectrum – is it centralized, with management across the enterprise, or is it decentralized, managed separately across various business units. Or a hybrid?

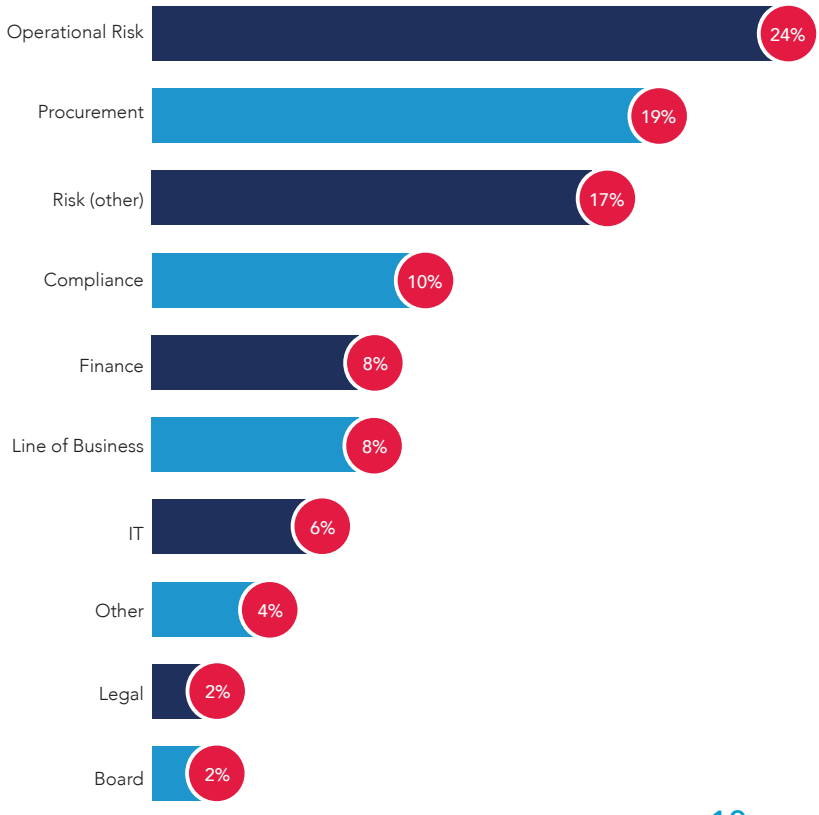
And, of course, a vital part of success for any TPRM program is its resourcing. Does the organization invest enough for it to deliver on the objectives of the organization? Is there enough funding for people, technology and innovation?

Finally, how are those responsible for managing third party risk being compensated? As a relatively new discipline, being populated by people from a variety of different functional backgrounds, there's a paucity of published data on salary for third party risk professionals. Salary can be a leading indicator of maturity – is third party risk a valued function within the organization – and does compensation reflect this?

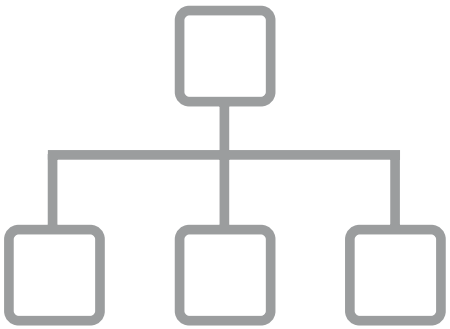
Where is third party risk located and managed?

An interesting aspect of the development of third party risk as a discipline is the fact that, historically, organizations have differed significantly as to where they house the function in their corporate structure. In practice, this has meant that third party risk teams have had differing priorities, policies and procedures – depending on the nature of the larger department they sat within.

Financial services regulators are making it clear that they wish to see third party risk aligned with the overall enterprise risk management function. So, it's perhaps not surprising that the survey shows that respondents – 79% of which were from financial services firms and insurers – are opting to house third party risk teams within operational risk (24%) and risk (other) (17%).



Of the total respondents, 19% of organizations still sit third party risk within procurement/sourcing. This percentage was boosted by the practices of non-financial firms, who are not under the same regulatory pressure to align TPRM with enterprise risk management. In the survey, 24% of non-financial firms placed the TPRM function within procurement/ sourcing, while 20% placed it within the finance team. Some 20% put it within risk (other).



Who has primary accountability for third party risk in your organization?

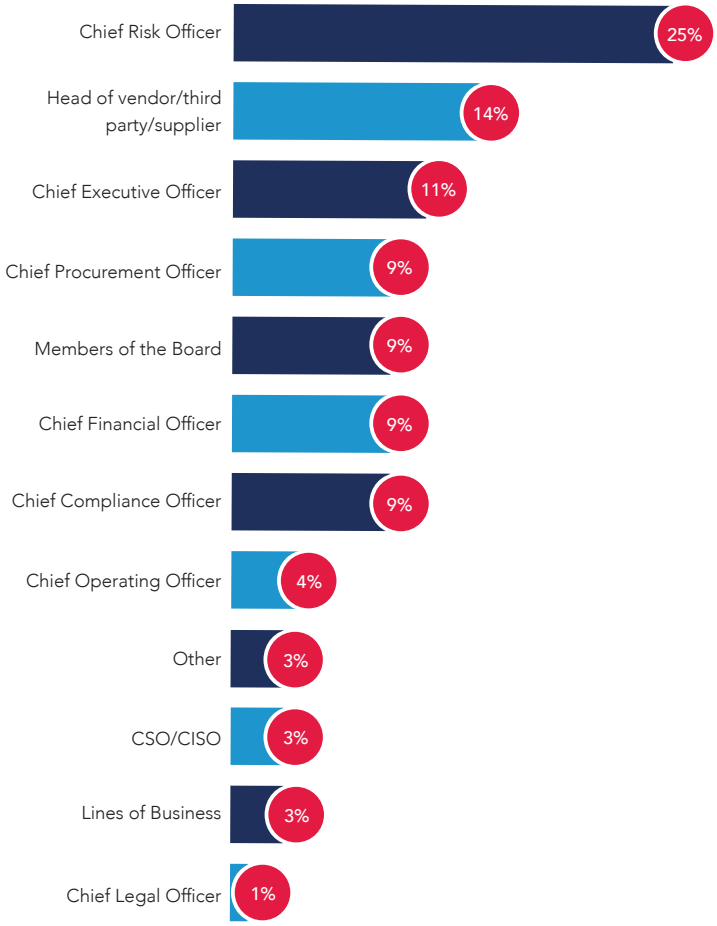
Given that TPRM can be housed in a variety of locations within a corporate structure, it's not surprising that primary accountability also takes many forms – responses show a degree of fragmentation across a variety of roles.

However, the results do illustrate that in most businesses, the C-suite and the board hold ultimate accountability for TPRM – four out of five of respondents reported accountability at these levels.

More broadly speaking, it's also likely that third party risk is being lifted up the board and senior management agenda due to the dynamic and rapidly evolving risks associated with cyber-security. Data breaches, cyber-attacks and ransom-ware all can have significant reputational and financial impact on an organization, and good boards will be interrogating practices across the extended enterprise relating to these issues.

Regulators are expecting firms to align their TPRM program with enterprise risk, which could be a reason why one-quarter of respondents say their chief risk officer (CRO) has primary accountability.

Some supervisory authorities also have an explicit expectation of board responsibility for reviewing TPRM policies and procedures. This could be driving the combined 20% who said the chief executive officer (CEO) or the board held this responsibility in their organization.



"An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution."

FDIC Guidance for Managing Third Party Risk

Decentralized vs. Centralized

The centralized model of TPRM has gained clear ascendency, according to the survey results. The largest proportion of respondents had a centralized in-house function (38%), followed by those who had a hybrid approach that was primarily centralized, but with some elements still managed in a decentralized way (31%). A further 14% were currently decentralized, but were moving towards a centralized model.

Just 15% of respondents said they were operating a decentralized model within their organizations. Outsourcing of the entire TPRM function – while being discussed within the discipline – is being practiced by just 1% of firms, with another 1% moving towards an outsourcing arrangement over the course of 2018.

- Centralized in house function (1)
- Decentralized in-house (3)
- Completely outsourced (5)
- Hybrid - primarily centralized, but some elements still managed in a de-centralized way (2)
- Hybrid - primarily decentralized, but moving towards a centralized model (4)
- Other (6)

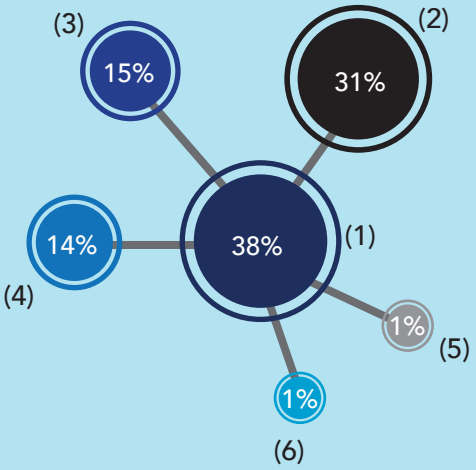
The Maturity Factor

Once again, financial services firms may be driving the trend toward centralization, because of regulatory requirements for central oversight of TPRM as part of an enterprise risk function. However, there are signs that centralization is now regarded as best practice, rather than as an alternative, equally valid, operating model. Three-quarters of those who had self-identified their program maturity as optimized or established have a centralized model – selecting either the centralized or hybrid, primarily centralized, answer options.

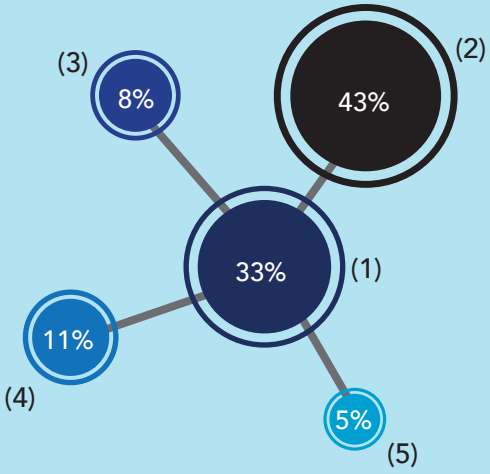
On the other hand, of those who self-identified their program as less mature (in the initial or developing phase), some 58% said they were running either the centralized or the hybrid, primarily centralized, models. A much greater proportion of less mature programs had a completely decentralized model – 22%. Just 8% of mature programs indicated they had opted for a decentralized model.

*More mature respondents were those that had self-identified as optimized or established. Less mature respondents were those who had self-identified as initial or developing.

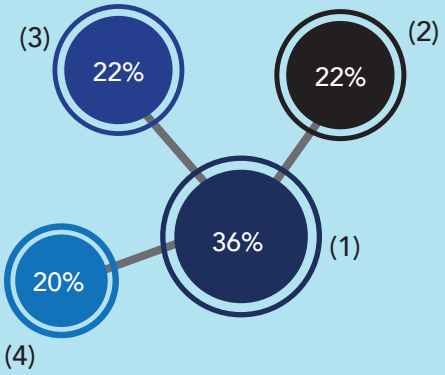
All respondents



More mature* respondents



Less mature* respondents

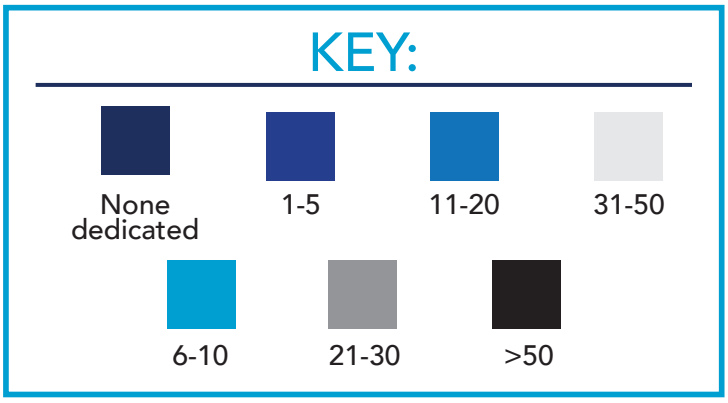


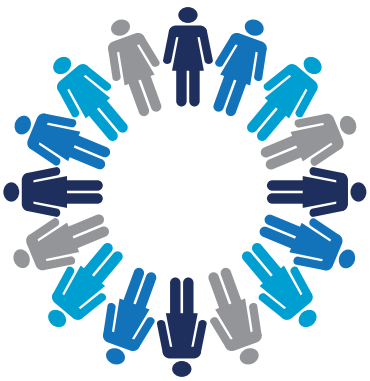
Size of Third Party Risk Teams

Interestingly, more than one-quarter of respondents said they did not have a dedicated TPRM team in place. Firms that self-identified as having less mature TPRM frameworks were much more likely (48%) to also report not having a TPRM team, as opposed to firms who said they had more mature frameworks (9%). Organizations with less than $25 billion in assets under management were also much more likely to say that they did not have a dedicated TPRM team (38%) than organizations with more than $25 billion in assets under management (15%). It is possible that organizations who said they did not have a dedicated team in place spread TPRM responsibilities across the corporate structure, assigning them to individuals who have other responsibilities as well.

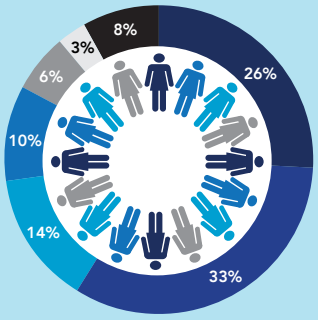
Overall, one-third of respondents had dedicated teams of between 1-5 people. Interestingly, this level of human resources was consistent for both more and less mature organizations. However, when looking the results by size of firm, firms with less than $25 billion in assets under management were more likely to have teams of that size than larger firms (40% v. 20%).
Among all respondents, nearly one-quarter had between six and 20 people dedicated to TPRM. More mature (28%) and larger firms (34%) were more likely to have this level of resource, compared with less mature firms (13%) and firms with less than $25 billion assets under management (16%).

More mature (20%) and larger firms (20%) were also far more likely to have human resource levels of 30 people or more. Some 14% of more mature firms reported having more than 50 people focused on TPRM.

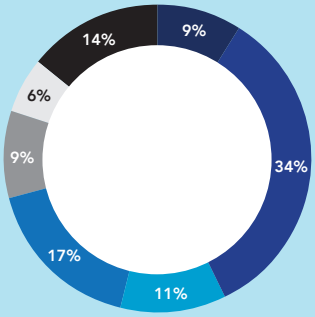




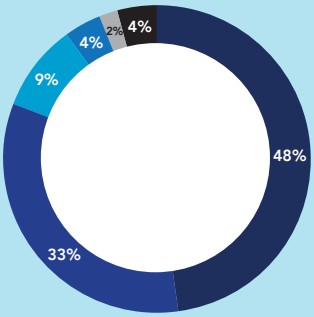
All Respondents



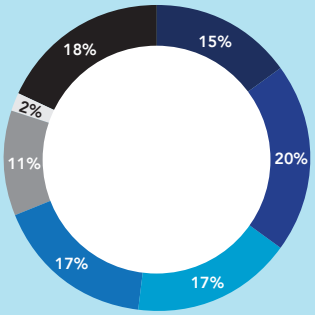
More mature (Optimized & Established)



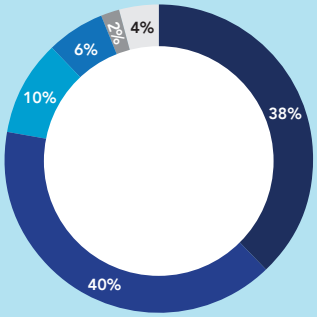
Less mature (Initial & Developing)



Over $25B Assets under management



Under $25B Assets under management

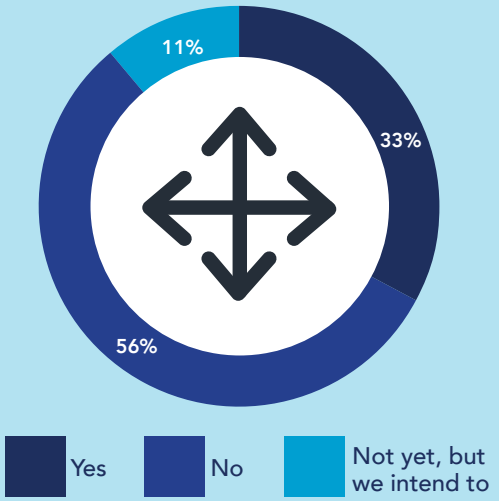


Outsourcing the TPRM Process

As TPRM matures as a discipline, organizations are finding they need to dig deeper into their third party relationships to better understand the risks that could potentially surface.

One-third of respondents now outsource some element of their TPRM program today, while another 11% said they intend to do so – showing that this emerging trend is gathering momentum.

Are you outsourcing any part of your third party risk management processes to shared services or managed services operations (e.g. validation, due diligence, etc.)



Budget

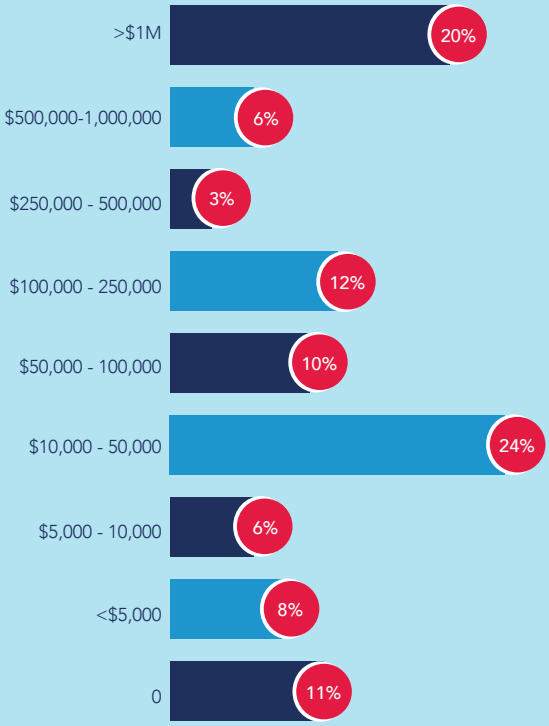
It is often said that the sign of a mature function in an organization is one that has its own budget responsibilities. In that sense, TPRM still has some way to evolve. Nearly four in 10 respondents did not know what the TPRM team's budget was, outside of headcount.

Of those who did know what their budget was, almost half (49%) had budgets less than $50,000, 10% had budgets between $50,000-100,000 and 41% had budgets over $100,000.

However, there were some relatively well-funded organizations, with 20% indicating that their budgets were in excess of $1million.

When considering investments required – for technology, third party risk intelligence content as well as audit – these budgets appear low, although conceivably these expenses could fall in other budget lines across the organization, such as IT and information management.

Approximately how much budget (US$) outside headcount does your organization have for third party risk management?



There was a positive correlation between budget size and maturity.

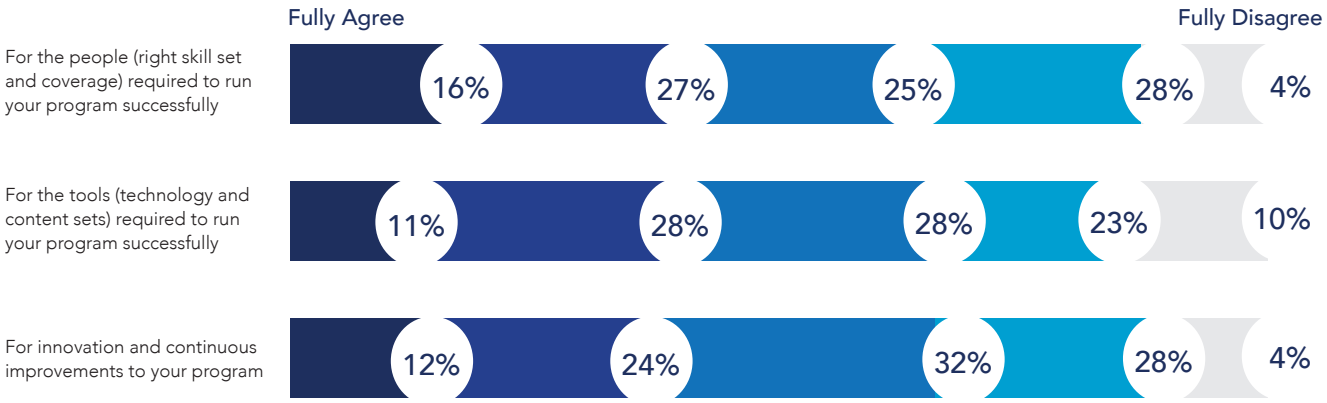
Level of Funding

In relation to budget, 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.

One-third of TPRM teams do not feel they are adequately resourced, and these tend to be the less mature teams. There was a relatively even split between those who felt they had adequate funds and those who did not. Those feeling a lack of funding were consistent across all three categories.

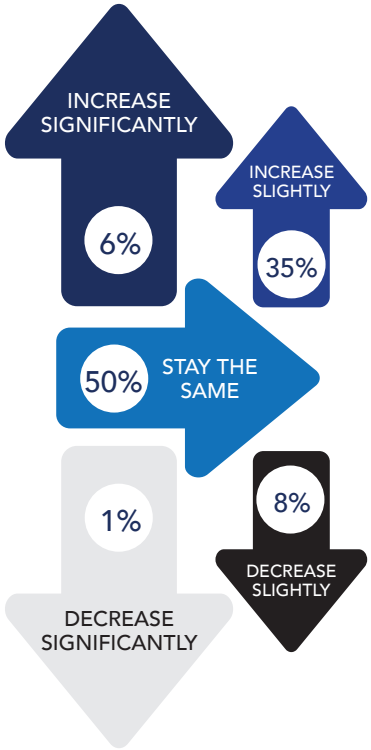
- 43% felt they were adequately funded for people (strongly agree/agree), 32% did not feel they were (strongly disagree/disagree).
- 39% felt they were adequately funded for tools (strongly agree/agree), 33% did not feel they were (strongly disagree/disagree).
- 36% felt they were adequately funded for innovation/continuous improvement (strongly agree/agree), 32% did not feel they were (strongly disagree/disagree).

On a scale of 1-5 (1 being 'fully agree' to 5 being 'fully disagree'), do you consider your third party risk management program has the right level of funding?



Annual Budget

Four out of 10 respondents are expecting to see increases in their TPRM budgets for the next 12 months, and half of respondents say that the budget will remain the same. Given the margin pressures that many organizations – and, in particular financial services firms – remain under, this level of financial focus on TPRM underscores the importance the discipline is beginning to attain. Only 9% of respondents are expecting to see their TPRM budgets decrease.



Annual Salary

While asking for annual salary figures is sensitive, salary can be a leading indicator of maturity. Is TPRM a valued function/role within the organization and does compensation reflect this?

While the majority of respondents chose not to answer this question, 37 did, which provides an interesting sample to reference.

Respondents were asked their total salary (base plus any bonus/benefits) and the currency for the salary figure. This allowed us to convert and standardize to $US. This is fairly broad-brush, and does not take into account variables such as city location, years of experience etc. which all play into salary outcomes. However, it is a starting point to learn from, and potentially draw some assumptions.

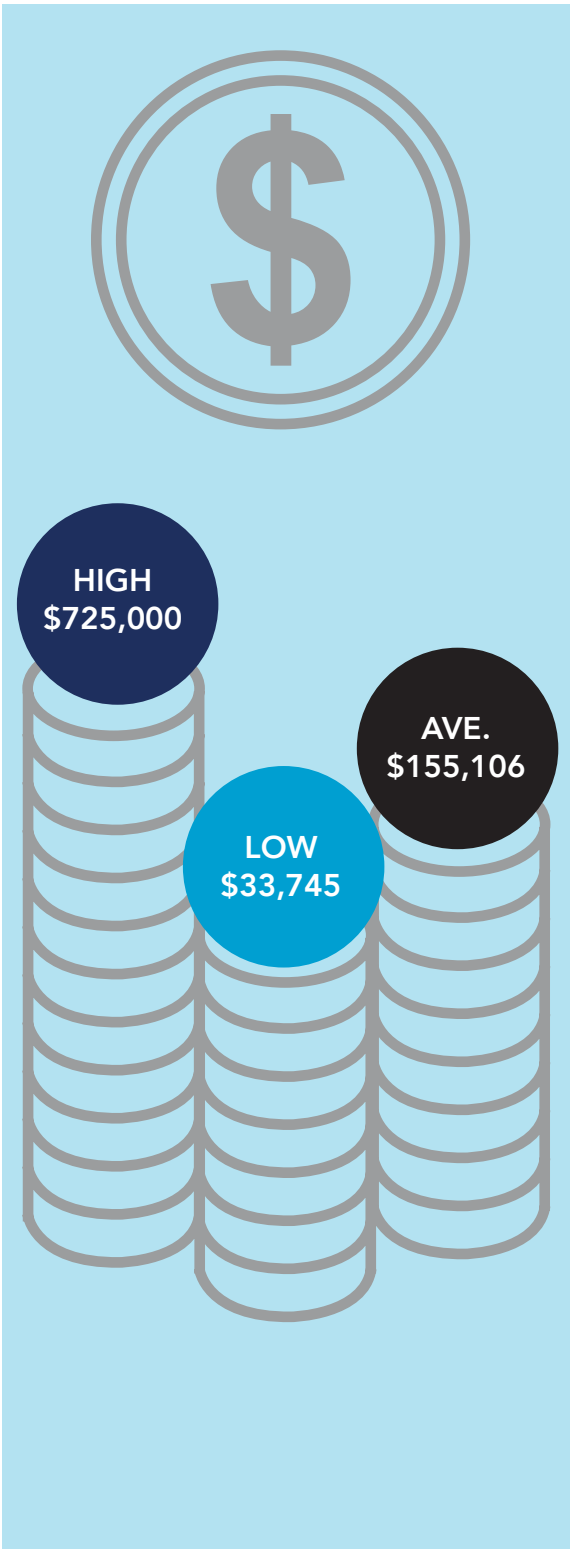
The range was $33,745 for a risk manager in Ghana for a financial services firm with $1B-1.99B in assets under management, to $725,000 for a director of vendor risk management in the US in a financial services organization with $500M-999 in assets under management.

The overall average compensation package was $155,106. Specific averages by job levels were:

Manager level: $75,119
Analyst level: $118,037
SVP/VP/Director level: $199,648

A positive correlation was observed between salary and maturity level, where higher salary earners tended to select 'established' or 'optimized' as the level of TPRM maturity in their organization.

The strength of the analyst salary could reflect specialized IT skills, particularly around cyber risk, information security and data privacy issues. It could also reflect advanced quantitative modeling skills – higher salaries for these skills are often seen in risk management-based teams.



A positive correlation was observed between salary and maturity level, where higher salary earners tended to select 'established' or 'optimized' as the level of TPRM maturity in their organization.

OBSERVATIONS

How TPRM teams are being structured and resourced provides important clues to how the discipline will evolve in the next few years. Certainly, these results show that TPRM is being taken seriously at most organizations, but that it faces a long climb uphill in terms of resourcing. The results of this portion of the survey show:

- **TPRM is still maturing as a discipline** – which means the survey shows TPRM located within various departments, and with a range of accountable stakeholders. The number of teams located within the risk management or operational risk teams suggests that regulatory pressure for this structure within financial services is having some influence, and possibly that it is beginning to be regarded as best practice.

- **Organizations appear to be gravitating towards a centralized model for TPRM** – this would allow it to align with other enterprise-wide risk management functions and processes, such as working with a risk appetite statement.

- **Resourcing is at a wide variety of levels** – however, the more mature programs are better resourced. This could be expected to plateau at some point as efficiencies are introduced.

- **Around a third of companies do not feel they are adequately resourced for their programs** – these tend to be the less mature, and so their TPRM teams may be concerned about the scale of the challenge ahead. However, budgets are set to either stay the same or grow at the majority of organizations.

- **Salaries for TPRM teams do not seem to be out of line with overall expectations** – analyst salaries are higher than managers, on average, and this may be due to specific specialisms that these individuals have, particularly around analytical or technical skills.

So, from these results, it's clear that TPRM has taken the first strides in its journey towards maturity as an established risk discipline within most organizations, and that while resources may always seem insufficient given the challenge at hand, it's encouraging that budgets are either staying the same or growing at most organizations. Additionally, compensation for TPRM executives seems healthy. Overall, these are positive signs for this nascent discipline.

PART 3: THIRD PARTY UNIVERSE AND PROGRAM

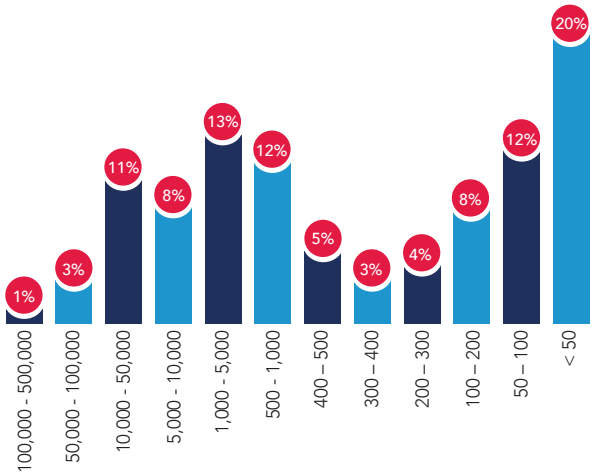
This section of the survey explores the mechanics of third party programs.

Questions focused on what types of activities organizations are undertaking, what kinds of risks they are managing within TPRM, and how they are approaching technology. The results show a wide range of maturity among respondents, with opportunities to improve across a number of key practice areas.

How many third parties does your organization work with?

More than one-third of the respondents work for organizations that have 1000 or more third parties, underscoring the growing complexity of the TPRM environment as more firms partner and outsource operations to enhance their performance. Of this total, 13% have between 1,000 and 5,000 third parties, while 11% have between 10,000 and 50,000.

Nearly two-thirds of firms operate with less complexity, saying they have 1000 third parties or fewer. Some 20% of respondents said they had 50 or fewer third parties.



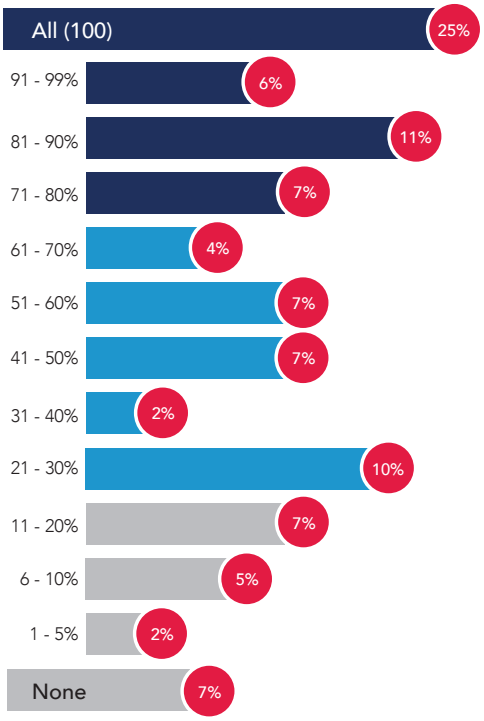
What percentage of third parties are maintained in a single inventory?

For third party risk management, base camp on the climb to best practice is having all of the firm's third parties in a single inventory. However, a significant portion of respondents – 22% – did not know if such an inventory existed in their organization.

Of those that did know, 40% had less than half of their third parties managed and maintained in a single inventory. Some 7% said that none of their third parties were collected in a single inventory. Overall, just one-quarter maintained all of their third parties in a single inventory.

Managing third parties via more than one inventory is inefficient, usually duplicative, and almost always involves manual work – quite possibly making this process a source of risk in its own right. Multiple inventories also have repercussions for other elements of TPRM, such as reporting.

These issues with multiple and incomplete inventories have led US regulators like the OCC to make it clear that they expect the financial services firms that they regulate to have a single, full inventory that captures all of their third party relationships.



"Proper documentation and reporting facilitates the accountability, monitoring, and risk management associated with third parties and typically includes...a current inventory of all third party relationships, which should clearly identify those relationships that involve critical activities and delineate the risks posed by those relationships across the bank."

OCC BULLETIN 2013-29

What percentage of third parties are critical?

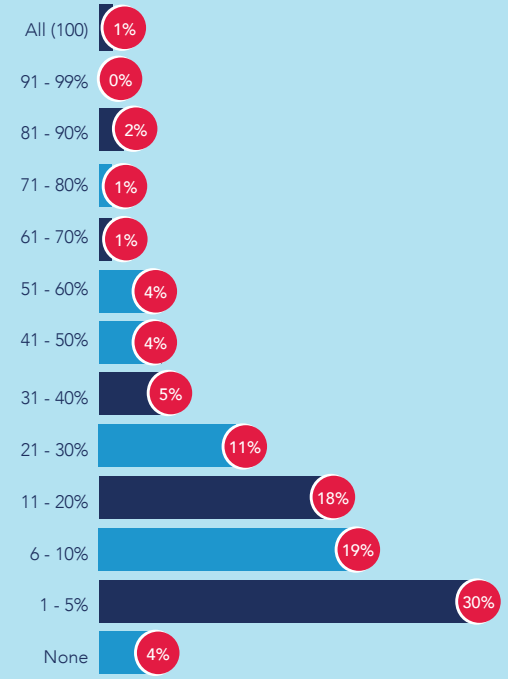
The next step for most firms who are building a TPRM program is to identify which third party relationships are critical to the business – regulators such as the OCC also require this.

Surprisingly, once again a significant number of respondents did not know who their critical third parties are – 17%.

Of those which did know the proportion of their third parties considered to be critical, three out of ten said that between 1% and 5% of their third parties were classified this way.

Rather surprisingly, 9% of respondents said that more than half of their universe of third parties were categorized as critical.

> *"A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships."*
>
> *OCC BULLETIN 2013-29*

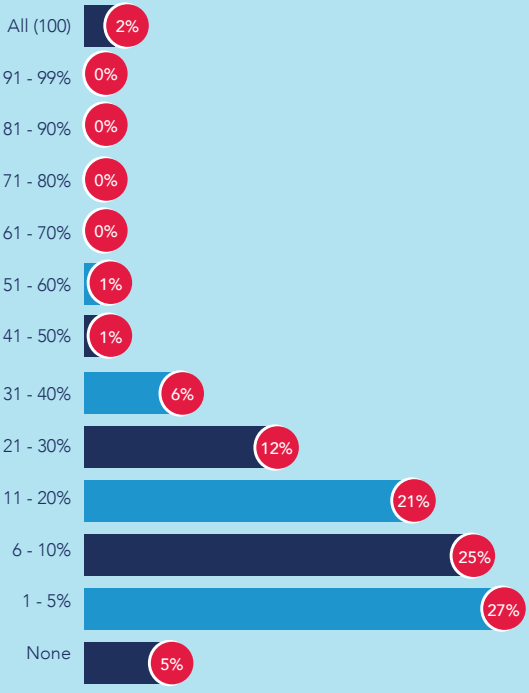


What percentage of third parties are classified as high-risk?

Once again, a significant proportion of respondents did not know the answer to this question – 19%. Of those that did know, nearly three-quarters of respondents indicated that between 1-20% of their third party universe could be categorized as high risk.

Others drew the boundary more broadly – 19% of respondents said that between 20-50% of their third parties were classified as high risk. Proportionally, results were similar to those of the critical third parties question, which could indicate that firms find their critical relationships to be their riskier ones.

> *"Due diligence and third-party selection: Conducting a review of a potential third party before signing a contract helps ensure that the bank selects an appropriate third party and understands and controls the risks posed by the relationship, consistent with the bank's risk appetite."*
>
> *OCC BULLETIN 2013-29*



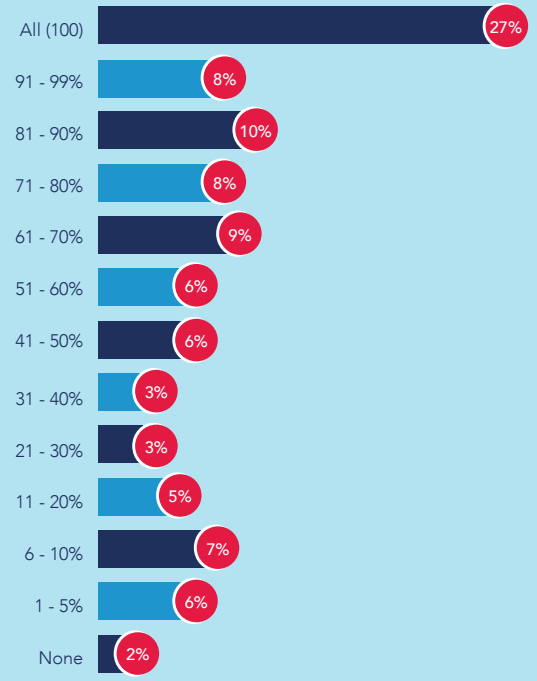
> *"Of particular relevance is whether or not the function being outsourced is considered critical or important, whether it is material outsourcing, or for authorised payment institutions and authorised electronic money institutions whether it relates to important operational functions."*
>
> *FCA's FG 16/5 - Guidance for firms outsourcing to the 'cloud' and other third-party IT services*

What percentage of third parties have initial due diligence conducted on them?

Just 27% of respondents said their organization had conducted initial due diligence on all their third parties. Clearly, organizations are struggling to implement due diligence policies across the board, or they are having difficulty getting due diligence performed on existing relationships. Yet, performing this initial due diligence is the second stage of the OCC's lifecycle of third party risk management – and therefore a key element of any TPRM program.

Many organizations appear to be making an effort to capture all of their third parties with an initial due diligence assessment. Some 26% say they have conducted initial due diligence on between 71% and 99% of their third party relationships.

However, many other organizations are struggling with this basic TPRM program component. Almost one-third of organizations have only conducted initial due diligence on 50% or fewer of their third parties.



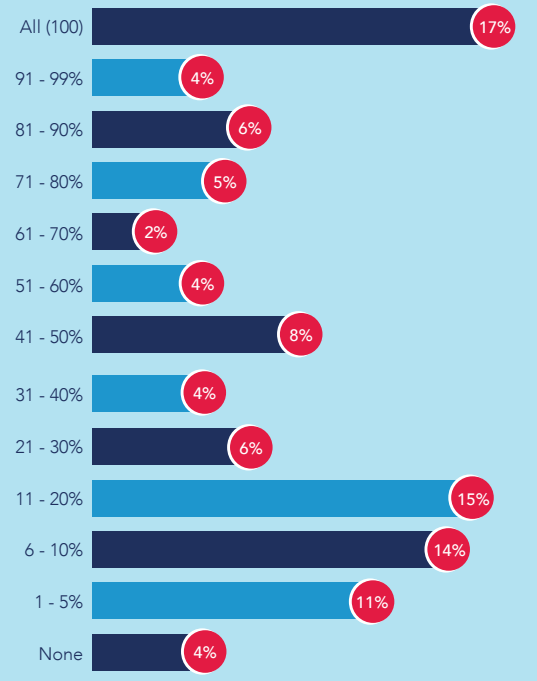
> *"The overall aim of the high-level regulatory obligations on outsourcing, and the detailed requirements that underpin them, is that a firm appropriately identifies and manages the operational risks associated with its use of third parties, including undertaking due diligence before making a decision on outsourcing. Our approach is risk-based and proportionate, taking into account the nature, scale and complexity of a firm's operations. Regulated firms retain full responsibility and accountability for discharging all of their regulatory responsibilities. Firms cannot delegate any part of this responsibility to a third party."*
>
> *FCA's FG 16/5 - Guidance for firms outsourcing to the 'cloud' and other third-party IT services*

What percentage of third parties have ongoing due diligence conducted?

Phase four of the OCC's TPRM lifecycle is ongoing monitoring of third parties.

However, the survey shows that an even smaller proportion of organizations are managing to conduct ongoing due diligence on all of their third parties – just 17%.

Nearly six out of ten organizations manage to perform ongoing due diligence on less than half of their third parties, and 4% are not conducting any ongoing due diligence at all.



> *"Ongoing monitoring: Performing ongoing monitoring of the third-party relationship once the contract is in place is essential to the bank's ability to manage risk of the third-party relationship."*
>
> *OCC BULLETIN 2013-29*

What risk types are managed for in your third party program?

- "Cyber risk and information security" has become a significant driver for third party programs; most likely in some part due to the proliferation of high profile breach cases that have generated headlines, regulatory sanctions, and business losses. A strong 86% of respondents said their organization was managing this risk type.
- Close behind, at 79%, was data privacy – again, likely driven by fear of reputational and financial loss at organizations. The implementation of the EU's General Data Protection Regulation (GDPR) – which has fines stitched right into the regulation itself – has also generated considerable interest in this area of risk.
- Compliance risk/regulatory risk also ranks highly at 77% – firms in highly regulated industries, such as financial services, have to ensure that their third parties meet the same levels of compliance for their processes as they themselves would have to.

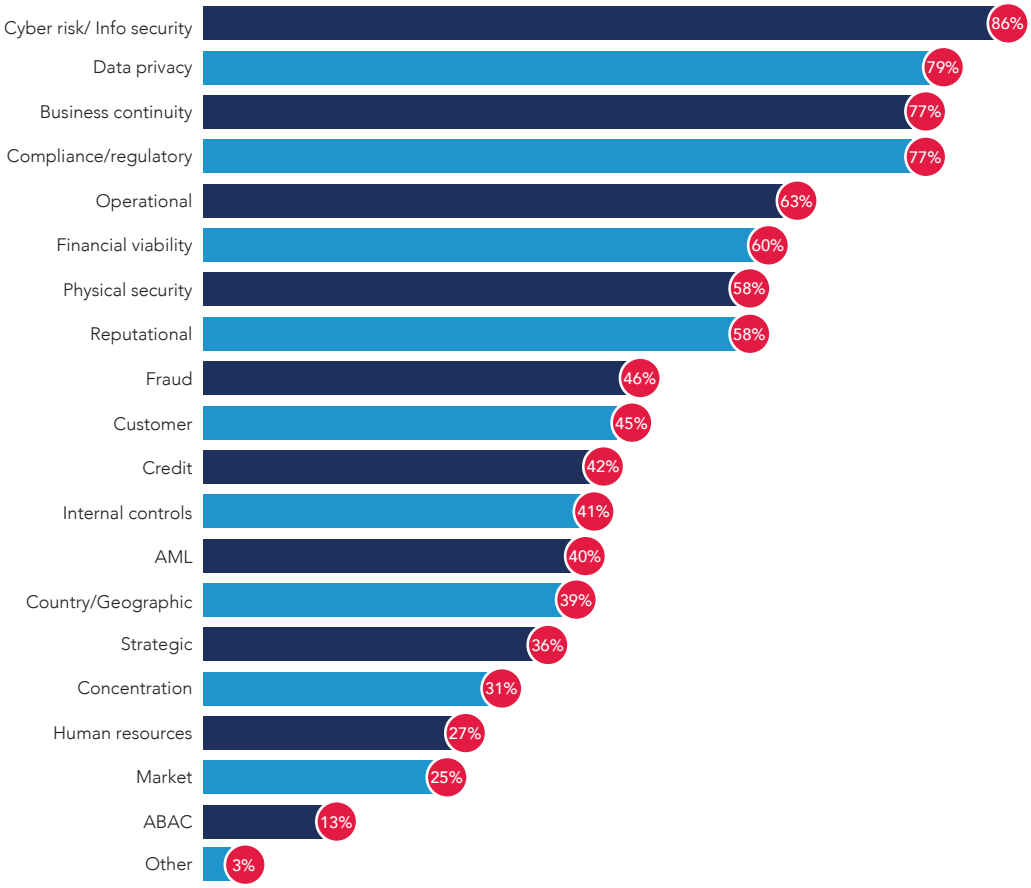
86% were managing cyber/information security risk in their programs

79% were managing data privacy risk in their programs

77% were managing compliance/regulatory risk in their programs

Overall, on average, organizations reported managing for nine risk types within their TPRM program, which is a broad spread. However, many organizations lack coverage of key risks that the OCC, in its guidance, says should be managed as part of standard practice. These include credit risk (58% do not manage this), strategic risk (64%) and reputational (42%).

Recently, regulators have begun telegraphing the importance of adequately managing concentration risk, but only 31% are managing this risk.. Anti-bribery and anti-corruption – a significant focus of both regulators and governments in many jurisdictions – is being managed by just 13% of programs.



> *"Operational risk continues to challenge banks because of increasing complexity of cybersecurity threats, use of third-party service providers, and increasing concentrations in third-party service providers for some critical operations."*
>
> *OCC Semiannual Risk Perspective for Fall 2017*

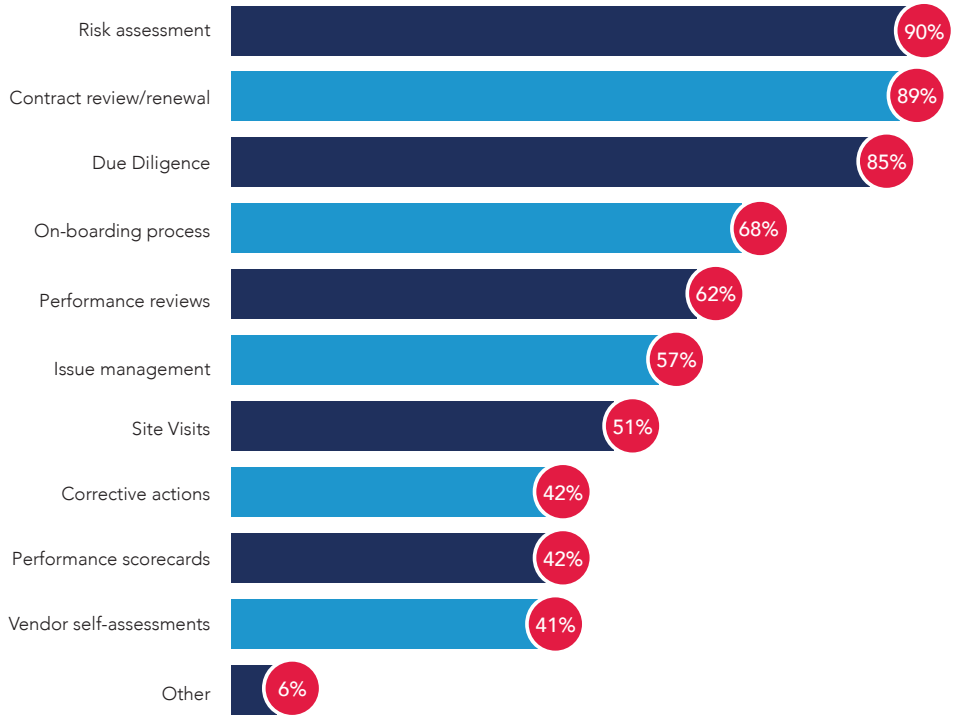
Which of the following processes does your organization use to manage third parties?

Nearly all firms are using risk assessments (90%), contract review/renewal (89%) and due diligence (85%) as processes to manage their third parties. These three components are essential to a TPRM program, and their use by firms reflects that these are a standard part of best practice that is also likely supported in the established legal contracting process.

However, other core TPRM processes are being used much less frequently. The onboarding process is used by only 68% of organizations, which perhaps signals a disconnect between third party risk and sourcing and procurement in some organizations.

Performance reviews are employed by just 62%. Issue management is performed by 57%, while site visits are undertaken by just over half of those responding.

Slightly more advanced TPRM processes show a further drop off in use. Corrective actions and performance scorecards are used by just 42% of organizations, while vendor self-assessments are performed by only 41%.



Other practices mentioned in response to this question show an interesting mix, including change management, reviewing 10K/10Q analyst reports, and onsite testing of controls.

OTHER

- External and internal audits
- 10K/10Q analysis of critical vendors
- Change management, in the form of material changes to a third party's control environment, or a continual assurance program for material outsourcing partners
- Outsourcing due diligence and renewal reviews
- Onsite testing of controls

Third Party Program Practices

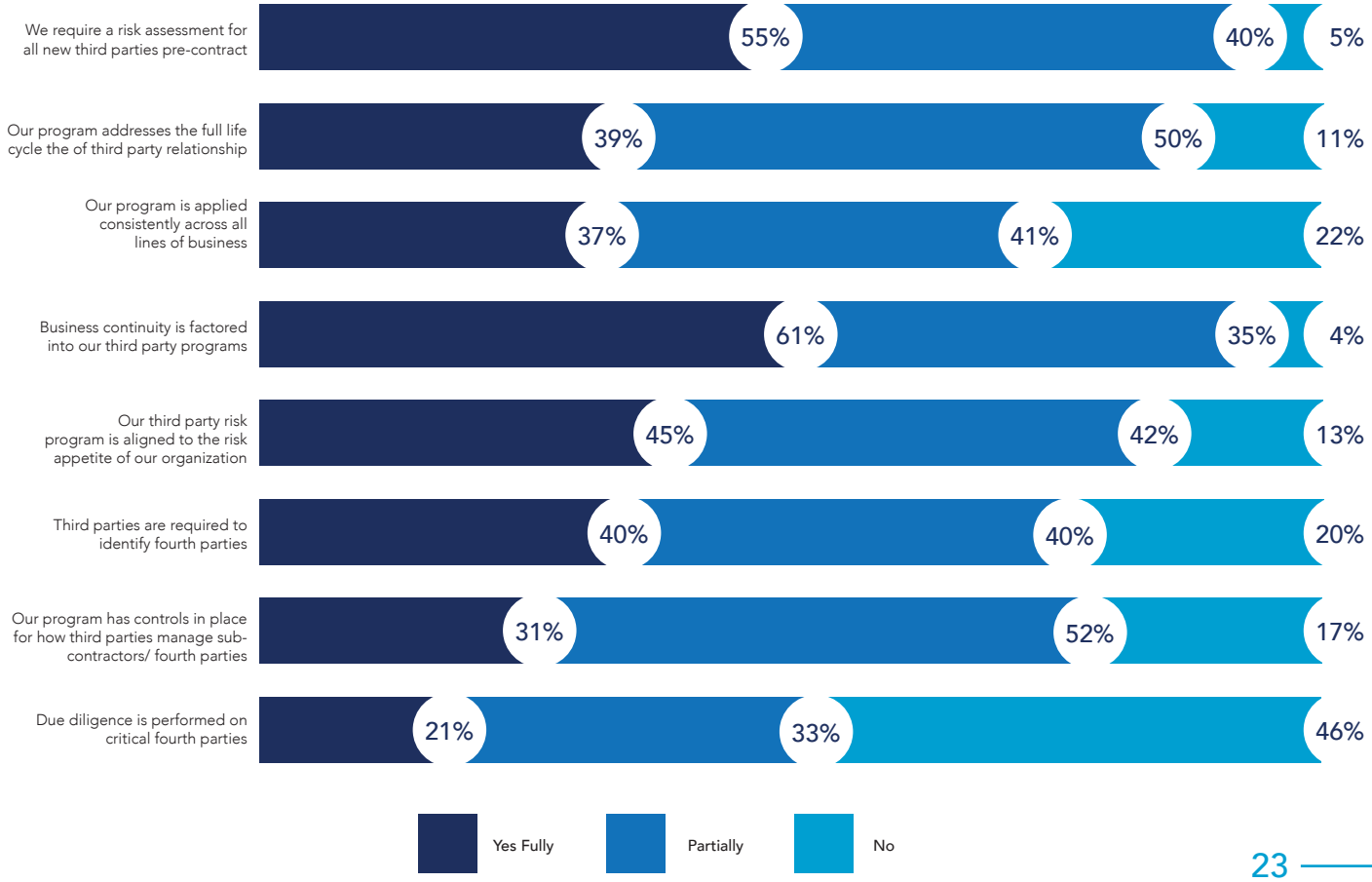
It's clear from the responses to this section that third party risk management programs are, developmentally, at a wide range of stages. Interestingly, business continuity is the most baked-in part of TPRM programs, with 61% of respondents saying this is fully implemented, and another 35% indicating that it is partly implemented. Just 4% have not tackled this as part of their TPRM program. The relatively advanced state of business continuity could be driven by regulatory demands at financial services firms, for whom BCP is a core requirement. It is also likely driven by business needs – during the contract negotiation stage for many outsourced processes, for example, BCP-related concerns would naturally be raised.

The second most implemented area in this survey question was risk assessments, with more than half of respondents saying that they required a risk assessment for all new third parties pre-contract. Another 40% of respondents indicated that this was a process they were implementing, although there are gaps. Only 5% did not perform assessments at all, which is in line with the percentage of respondents who said they were only in the initial stages of implementing their TPRM program at their organization. For most organizations seeking to put in place a TPRM framework, assessments of vendors and partners is a natural initial step.

Other elements of organizations' approach to TPRM are still evolving. Only 45% of respondents say their TPRM program is fully aligned to the risk appetite of their organization, while just 39% completely address the full lifecycle of the third party relationship within their framework. Only 37% say their organization applies the TPRM program consistently across all lines of business.

Oversight of fourth party relationships is also an area that organizations need to develop further. Only 40% stated that third parties are always required to identify fourth parties, while 31% of respondents reported having controls within all of their third party relationships for the management of fourth parties. Just 21% say they always conduct due diligence on critical fourth parties. Some 46% do not conduct due diligence on critical fourth parties at all.

Please indicate how these statements reflects the third party program you have in place in your organization:



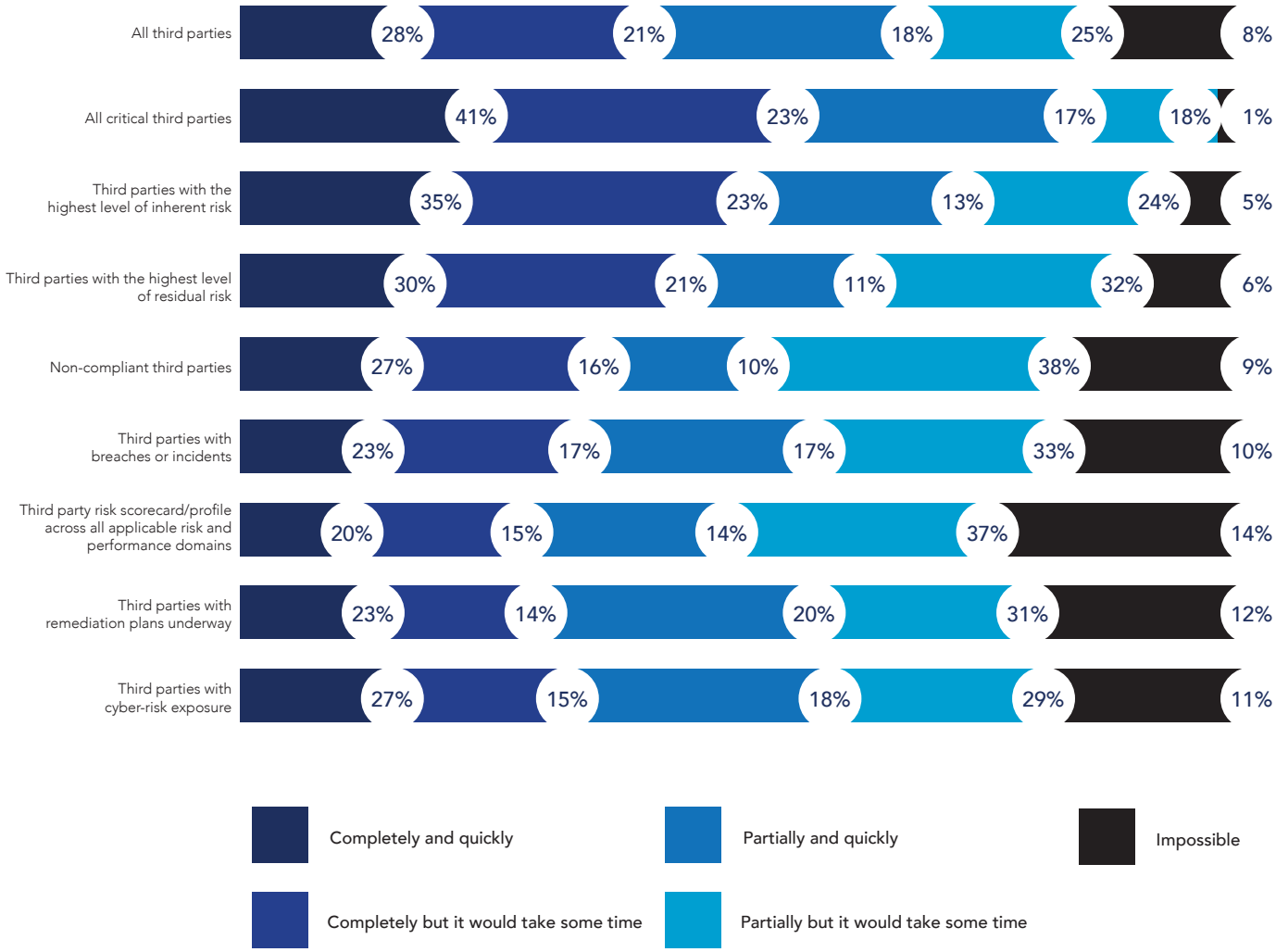
Reporting

It's clear from the responses to this question that organizations are struggling with reporting when it comes to third party risk management.For example, only 41% of respondents can produce a list of their critical third parties quickly and easily. Just 28% can produce a list of all of their third parties quickly and easily. For regulators – as well as those within the discipline – the ability to produce such lists is a basic requirement of any framework. This will also be an area of board focus, as they require timely and accurate reporting for oversight and governance.

Some 38% of respondents would struggle to – or not be able to – produce a report on the residual risk in their third party relationships. Some 47% would encounter the same level of difficulty in generating a list of non-compliant third parties, as would 43% trying to report on third parties with incidents or breaches. One in four would struggle or not be able to produce a report on third parties with cyber risk exposure – despite the significant regulatory and business focus on this issue.

The report that respondents would struggle with the most is a third party risk scorecard/profile across all applicable risk and performance domains. Just 20% of respondents could do this completely and quickly. More than half of respondents would either struggle or not be able to produce this report at all.

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



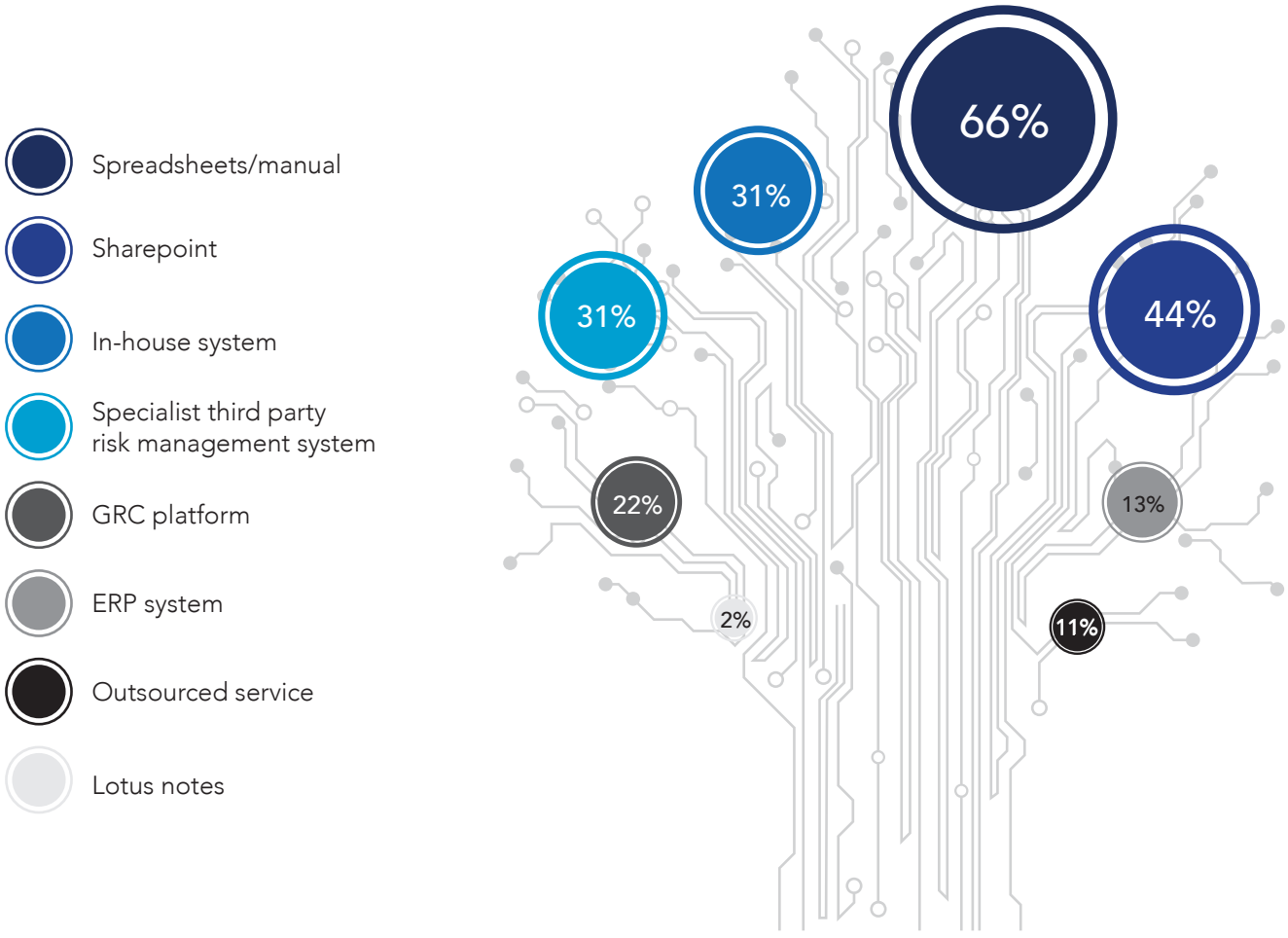
What technology/tools does your firm use to track and manage your third party risk processes?

Organizations use a wide range of tools and technologies to track and mange their third party risk processes.

The most common was spreadsheets (66%), followed by Sharepoint (44%). While these tools are inexpensive, as they exist on nearly all desktop software packages, the predominance of their use may well account for the difficulty that organizations face with their TPRM reporting requirements. Using manual solutions such as these are human resource intensive, and usually require more time and other corporate inputs to perform basic TPRM tasks. In addition, these manual solutions are not able to produce an audit trail to the standard that regulators are now insisting on in some jurisdictions.

Other systems include utilizing ERP systems for TPRM, which 13% of respondents are doing, and using Lotus Notes, which 2% depend on. Some 22% of organizations are using their internal GRC solutions, even though these software packages often do not include all of the elements necessary to conduct TPRM effectively. These shortcomings were highlighted when participants were asked about technology challenges.

However, a substantial minority of organizations - 31% - are using a specialist third party risk management solution. Another 31% are using in-house solutions for their TPRM programs. In this question, 11% said they were using an outsourced service specifically to track and manage their third party risk processes.



Greatest Technology Challenges

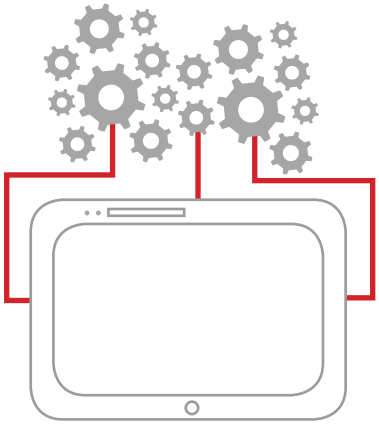
Respondents were asked an open-ended question: "What are your greatest technology challenges?" These were then grouped by theme and the number of mentions noted.

The top technology challenge for TPRM teams was the limitations of the current system in use.

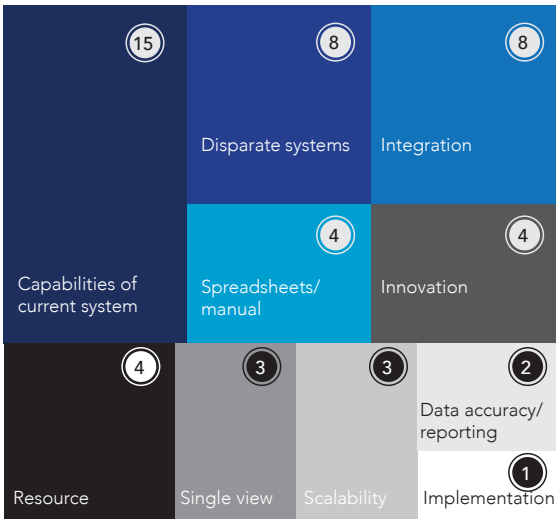
Says one respondent, the *"current GRC Tool is sub-optimal."* Respondents with last-generation GRC or in-house solutions struggle to keep up with basic requirements for third party management, which is only exacerbated by the change dynamics associated with regulation and risk. One organization is challenged by the *"limitations of the in-house system as changes and updates cannot be done instantaneously, and the type of change is also limited."* Another cited the lack of *"ability to quickly make changes to the GRC tool as well as retain staff to support."* These individuals, and others, are also finding it difficult to make the necessary changes to their software, to keep up with TPRM regulatory demands. One respondent says the challenge their organization faces is the *"development of a system that has the flexibility to manage the ever-evolving requirements (regulators, markets, products) that we face when managing our vendors."*

The second biggest technology challenge is the disparate systems that many TPRM teams are having to contend with – both within their own function and across the business.

One respondent stated their TPRM team has to make do with *"multiple systems, a lack of integration, and outdated technology that does not keep up with the compliance environment."* Another writes that the *"maturity"* and *"dispersed"* nature of the risk systems makes *"data modeling very complex."* A third respondent was critical of the fact that the TPRM team has to use different tools across the enterprise that are *"inconsistent across affiliates."* A fourth respondent notes that the multiple systems make it difficult to consolidate information and have the "golden sources" of data that regulators now require.



Mentions by theme



> *"...the development of a system that has the flexibility to manage the ever-evolving requirements (regulators, markets, products) that we face when managing our vendors."*
>
> *Enhanced Due Diligence Manager, asset management firm, greater than $100B assets under management, UK.*

> *"Limitations of the in-house system as changes and updates cannot be done instantaneously, and type of change is also limited."*
>
> *Associate Director, Monitoring & Compliance - Third Party Risk, bank, $25-50B assets under management, Canada.*

> *"Multiple systems, lack of integration, outdated technology that does not keep up with compliance environment."*
>
> *Supplier Governance Advisor, bank, greater than $100B assets under management, USA.*

> *"Current GRC tool is sub-optimal."*
>
> *Director, Third-Party Risk Management, technology firm, $30B-60B revenues, USA.*

Integration is tied for second place, in terms of technology challenges for organizations.

Respondents complained of "no linkages across various systems" as well as a lack of "connections between Accounts Payable and the GRC platform." Another respondent said they wished their system connected to legal as well. Workflow was also seen as part of the integration challenge, with respondents citing a need for workflow to connect these different parts of the organization as part of the TPRM process.

Spreadsheets/manual, innovation and resources all tied for fourth place.

- Spreadsheets were seen as challenging because of the lack of ability to connect the data in the way that a relational database can.
- Innovation is a significant challenge as organizations grapple with new technologies within the business, as well as cyber risks and data security issues.
- More resources are on the wish list of many TPRM teams, including the budget to implement a new technology solution, as well as the staff to support it.
- Having a single view, scalability, and data accuracy/ reporting were also key technology issues cited by respondents.
- Being able to have a single view of TPRM data – one source of truth – is a key challenge that organizations are facing, often hampered by disparate systems and a lack of integration.
- Scalability is a source of concern as organizations struggle with managing "the size and quantity of documentation received from third parties" as well as complex corporate structures within their current TPRM technology arrangements.
- In line with the results that demonstrated the difficulty for many organizations to extract even simple reports, obtaining "accurate data on third party performance across different metrics" and providing "customized reporting" were identified as technology-related challenges by participants.

> *"No linkage into other systems such as accounts payable and legal. No workflow for assessments."*
>
> *Head of Third Party Risk, broker-dealer, Japan*

> *"Connection between Accounts Payable and the GRC platform."*
>
> *Vendor Risk Program Manager, bank, $10B-25B assets under management, USA.*

> *"Using a spreadsheet rather than relational database."*
>
> *Head of Third Party Risk, broker-dealer, Japan.*

> *"Money, legacy systems, attitudes, job security, in-sourcing/relocation."*
>
> *Head, Credit Policy and Risk Analytics, bank, $50B-100B assets under management, UAE.*

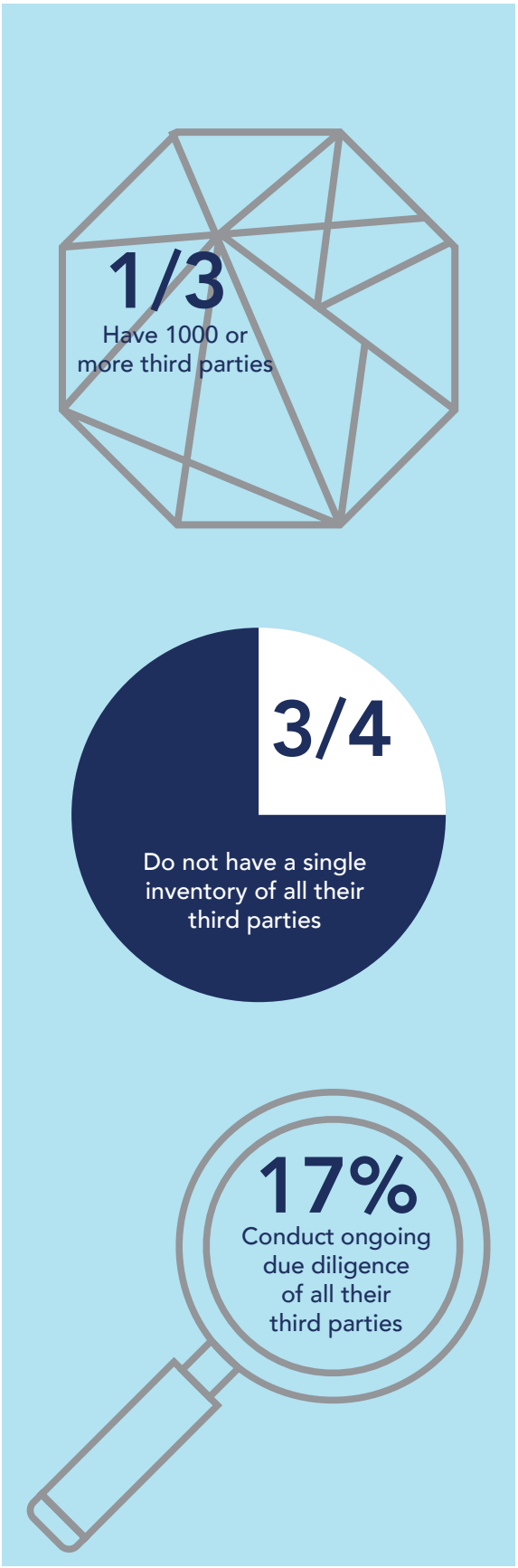
> *"Obtaining a single supplier view that meets all stakeholder requirements and prevents data duplication e.g. procurement, legal, IT, BC, CISO, Risk, etc."*
>
> *Resilience Manager, asset management firm, greater than $100B assets under management, UK.*

> *"Not a lot of systems that can handle our structure, size, etc."*
>
> *Senior Manager, Audit & Risk, asset management firm, $25B-$50B assets under management, USA.*

OBSERVATIONS

This section of the survey revealed that, among the respondents, there was a wide range of program sizes and levels of sophistication, but with some consistent challenges.

- One-third of the organizations surveyed have 1000 or more third parties - and for TPRM programs, with size also comes complexity. Scale and complexity may become increasingly problematic, especially given the types of technology deployed as well as resourcing at some organizations.
- Three-quarters of firms are currently not capturing all of their third party relationships in a full or single inventory.
- The percentage of third party relationships considered critical, or high risk, by organizations is relatively high. This underscores the increasing strategic importance of third parties and their role in what is beginning to be termed the "extended enterprise."
- Organizations are still putting into place key components of the TPRM lifecycle. For example, one third of organizations conduct due diligence on 50% or fewer of their third parties, and just 17% of respondents are conducting ongoing due diligence on all of their third parties. The nascence of the TPRM discipline can also be seen through the fact that less than half of firms are using corrective actions, performance scorecards, or vendor self-assessments.
- Although TPRM programs are putting significant focus on the risks regulators consider hot – such as cyber risk and data privacy – overall, many TPRM programs are managing a fairly wide range of risks.
- TPRM programs seem to be focusing on having BCP arrangements in place, as well as risk assessments. Other program elements are still evolving.
- Two-thirds of organizations use spreadsheets, and 44% use Sharepoint, to track and manage their TPRM processes.
- All of this adds up to a lack of adequate TPRM reporting at organizations – most firms cannot produce core TPRM reports completely and quickly.



In summary, the results of this section of the survey reveal that, at most organizations, there is considerable scope for the development of the TPRM program. Of all of the gaps, the state of TPRM reporting seems the most troubling – not just because of the underwhelming current state of play, but also because so much of the perceived value of TPRM by other stakeholders rests on the ability of the discipline to generate intelligence quickly and easily for use in business decision-making. However, across the board, TPRM teams need to work hard over the next 12-24 months to ensure all of their third parties are in a single inventory, that they are all risk assessed upon onboarding, and that due diligence is applied as part of their ongoing relationship.

PART 4: CHALLENGES & 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.

What do you think will be the greatest challenges ahead for third party risk management in your organization in the next 12 months?

There were a wide range of challenges articulated in response to this question – TPRM teams clearly have a lot to contend with as they embed and evolve their programs. Key issues included:

Delivering best practice – This broad theme captures a range of specific issues that teams are encountering, including:

- "Injecting new/enhanced SLAs into appropriate third party contracts (new or renewing)."
- "Identifying the critical and high-risk vendors and structuring a tiered program to address the supply chain risks."
- "Living up to best practice objectives in terms of 100% completion and monitoring."
- "Incorporate as ongoing activity instead of ad-hoc", as well as "tracking, consistency, better reporting."

Resource – Having adequate resources to support TPRM is an issue across a number of different areas, including headcount (recruitment and retention), funding, and the time as well as attention of the partners they work with inside the business, such as procurement.

Scale and speed of change – TPRM teams are having difficulty keeping up with the change that is all around them, including scaling up their programs, the growing number of third parties their business works with, and constant regulatory change. Teams are under pressure to deliver quickly within this dynamic environment.

- Working with suppliers such as outside law firms to complete TPRM tasks can sometimes slow things down.
- Business changes such as mergers and divestitures can mean that resources are focused in other areas.
- Working with non-traditional vendors such as open source, IoT, and FinTech incubator partners presents issues.
- Another challenge is "keeping up-to-date with changes in architecture and data in scope for each engagement."

Mentions by theme

> *"The program is not at the maturity level needed and required. The greatest challenge is the rapid growth of using 3rd parties, along with a more rigorous compliance environment and ensuring the risk to the department/ organization is mitigated."*
>
> *Supplier Governance Advisor, bank, greater than $100B assets under management, USA.*

Regulators and regulations – Respondents spoke of the challenges they are facing in keeping up with the pace of regulatory change around TPRM. One respondent summed this up, saying that they were challenged by "adapting to the ever-changing regulatory requirements and updating reporting and technology to ensure comprehensive tracking and reporting." Specific issues organizations are faced with include:

- GDPR compliance, which was specifically mentioned by several respondents.
- Proactive risk management as supervisory focus, rather than just control validations.
- Evidencing and reporting on TPRM programs to regulators, as well as senior management and the board.
- Staying on top of cybersecurity requirements.

Enterprise buy-in – "Gaining enterprise-wide participation" in TPRM programs is an issue for many organizations.

Says one respondent, "The greatest challenge ahead is to incorporate third party risk management goals into the goals of the first line of defense." Another says their organization is working to develop a "consistent understanding of risk and risk management techniques across a wide range of supplier managers." A third respondent says of their TPRM framework, "Development is in progress with a view to establishing a comprehensive framework. Challenges will be to embed this into the organization, including [the] establishment of roles and responsibilities." In particular, TPRM teams found it challenging to get buy-in from the first line of defense for the management of cyber risk and concentration risk.

> *"Regulators raising the bar on proactive risk management rather than control validations."*
>
> *Analytics Executive, bank, greater than $100B assets under management, USA.*

> *"Evidencing GDPR compliance to the satisfaction of the board."*
>
> *Head of Business Services, insurance firm $500M- $999M revenues, UK.*

> *"Understanding concentration risk through the third-party risk management supply chain, meaning that we need to understand our third party's third parties."*
>
> *Board member, bank, less than $1B assets under management, USA.*

> *"Change - constant change (merger/ divestiture) means key resource is concentrated in other workstreams."*
>
> *Strategic Procurement Manager SRM, asset management firm, greater than $100B assets under management, UK.*

> *"Full coverage of third parties other than traditional vendors (open source, IoT, FinTech incubator partners, etc.)."*
>
> *Chief Risk Officer, financial services firm, greater than $100B assets under management, USA.*

> *"Adapting to the ever changing regulatory requirements and updating reporting and technology to ensure comprehensive tracking and reporting."*
>
> *Sr. Director, bank, greater than $100B assets under management, Canada.*

> *"Coordination across different business lines."*
>
> *Head of Risk Management, insurance firm, $100M - $ 499M revenues, UK.*

What do you think will be the greatest opportunities ahead for third party risk management in your organization in the next 12 months?

On the flip side of the coin, respondents saw a wide variety of opportunities for third party risk management in the 12 months ahead.

Although regulatory pressures may be driving framework development, many respondents believe this investment will pay off for the business, too. Respondents talked about:

Gaining better insight and intelligence – Many respondents recognize that enhanced TPRM will deliver important intelligence to the organization which will enable them to make better business decisions about their third party relationships. One respondent said TPRM will deliver "better insight on true performance by third parties". Another said they were looking forward to "showcasing the true value from a vendor assurance program that is risk-driven and enables the business to see the value added." The following tools and techniques were specifically cited by respondents as driving this insight and intelligence:

- "Supplier self-service technology to provide insight greater than attestations"
- "Advanced reporting on third-parties in the same service category across risk domains and risk factors"
- "New risk management tools and methods and to offer data management and interpretation"
- "Analytics capabilities using machine learning is reducing manual efforts and providing better information faster"

Increased efficiency – Respondents who are deploying a new TPRM platform in the coming 12 months said they were looking forward to the increased efficiency that would result from this change. A key element was being "much more efficient in providing valuable insights to our execs for actions."

Consolidation and consistency – Respondents could see how TPRM would deliver clear benefits in terms of creating consolidation and consistency across the business. Said one respondent, "We are combining our Third Party Vendor (Suppliers) Program with our Partner (Business Relationships) Program. This will drive consistency." Another said their organization was consolidating other affiliate programs into the centralized TPRM program. Others were streamlining their vendor onboarding process, or their TPRM technology solution, and making it consistent across the company. Said one respondent, "we're bringing together all stakeholders involved in Third Party Management to produce a comprehensive and streamlined end-to-end process."

Mentions by theme

11	Increased insight and intelligence
7	Increased efficiency
6	Consolidation/consistency
5	Executive awareness
5	Other
5	Improved processes
5	Holistic/end-to-end/completeness
5	Culture/education/buy in
3	Technology
3	Industry
3	Standardization/collaboration
3	Rationalization
2	Expanded scope
2	Performance measures
2	Innovation
2	Strategic opportunities
1	Resilience
1	Security
1	Integration
1	Risk framework
1	Collaboration (internal)
1	Growth
1	Resource
1	Cost savings
1	Centralization
1	Demonstrate value add

> *"We are combining our Third Party Vendor (Suppliers) Program with our Partner (Business Relationships) Program. This will drive consistency."*
>
> *Analytics Executive, bank, greater than $100B assets under management, USA.*

> *"Bringing together all stakeholders involved in Third Party Management to produce a comprehensive and streamlined end-to-end process."*
>
> *Resilience Manager, asset management firm, greater than $100B assets under management, UK.*

> *"Move from vendor management to vendor performance measurement."*
>
> *Director, Enterprise Risk, bank, $2B-10B assets under management, USA.*

Executive awareness – TPRM teams see building executive awareness of third party risk management as a real opportunity for the coming year. Some said they already have "strong tone-at-the-top support to strengthen the third party risk and control activities." As a result, the next step is to "increase awareness and adherence to the program throughout the organization." Others said this year brings the opportunity to "raise the profile and awareness [of TPRM] at a strategic level."

Improved processes – Organizations which are implementing new third party risk management solutions over the coming year, in particular, were looking forward to "automation", "refining processes", "making TPRM more systematic," and "rethinking and digitizing entire processes and functions."

Holistic/end-to-end/completeness – Respondents saw opportunities and benefits in taking a more complete and holistic approach to their third party management. They reported that they were looking forward to having "100% of monitored vendor risk assessments completed," and "fully formalizing coverage across all vendors". Others said they were keen to achieve "greater clarity of strategic requirements and definition of an appropriate risk appetite that will support the development of a holistic third party risk program with the required investment."

Other areas that organizations are viewing as opportunities include:

- **Culture/education/buy-in** – This ranged from "selling the concept" of TPRM through to ensuring "continued acceptance of the program across the organization."
- **Industry standardization/collaboration** – Respondents are keen to embrace the wide range of industry initiatives that are forming, or evolving, in the TPRM space.
- **Rationalization** – Respondents see a key benefit of a good TPRM program as being able to better understand the context around different supplier relationships, with a view to rationalizing relationships across the organization.
- **Performance** – One respondent said their organization was going to be moving "from vendor management to vendor performance measurement." Another indicated that they would be "gaining better insight on true performance by third parties."

> *"Leaders who are now more educated and aware of the importance of management of 3rd party risk - increasing awareness and adherence to the program throughout the organization."*
>
> *Associate Director, Monitoring & Compliance - Third Party Risk, bank, $25B-50B assets under management, Canada.*

> *"Streamlining the onboarding process - unifying the process across the company."*
>
> *Assistant Vice President of Operations, financial services firm, greater than $100B assets under management, USA.*

> *"Advanced reporting on third parties in the same service category across risk domains and risk factors."*
>
> *Director, Third-Party Risk Management, technology firm, $30B-60B revenues, USA.*

> *"Clearly defining roles and responsibilities should identify efficiencies and effective risk management."*
>
> *EMEA Third Party Officer, bank, greater than $100B assets under management, USA.*

> *"Resolving endemic issues collaboratively."*
>
> *Social Accountability Director, consumer packaged goods firm, $30B-60B revenues, UK.*

> *"Rethinking and digitizing entire processes and functions."*
>
> *Head, Credit Policy and Risk Analytics, bank, $50B-100B assets under management, UAE.*

> *"Improved risk posture when a platform is deployed. This will also help us be much more efficient in providing valuable insights to our execs for actions."*
>
> *Senior executive, bank, greater than $100B assets under management, Canada.*

CONCLUSIONS

WHAT WE HAVE LEARNED

In summary, while the discipline of TPRM may still be in its formative stages, and it may have significant challenges ahead, results of this survey point to a real promise of opportunity for the discipline to deliver credible value to organizations. Key findings of the survey were:

- The majority of organizations are at a relatively early stage of their TPRM journey – two-thirds of respondents say their programs are developing, defined, or in the initial stages. Teams can be small, and available resources not wholly adequate for the complexity and change velocity that third party risk presents. However, nine out of ten respondents expect their budget to either grow or stay the same over the coming 12 months, signaling that most organizations – in these times of tight margins – are serious about establishing TPRM programs.

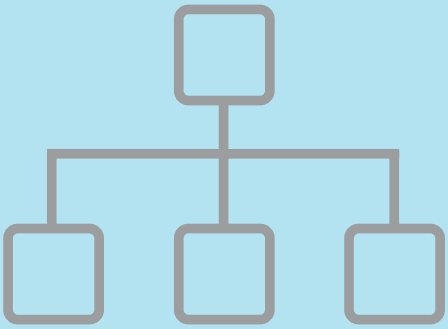
- While regulatory compliance is the primary driver for nearly half of organizations, business and cost benefits were the motivating driver for more than four out of ten respondents.

- Organizations are gravitating toward locating their TPRM function within the risk management team, and are using a centralized structure that aligns to the overall approach to risk management – examples of this include the use of risk assessments and development of a risk appetite. On average, programs are actively managing nine distinct risk types, which suggests that organizations are taking a holistic approach to risk management.

- While most firms manage risk for information security/cyber, data privacy, business continuity and compliance/regulatory, firms are lagging on other key areas of risk - notably, concentration risk, strategic risk and anti-bribery and anti-corruption (ABAC) risk.

- Only 39% of respondents reported that their program fully addressed the full lifecycle of third party relationships. Organizations are still struggling with some of the basic components of the lifecycle, such as capturing all third parties in a single inventory, conducting due diligence, and reporting. Many of these challenges are due to a lack of technology investment – two-thirds are using spreadsheets for at least part of their TPRM program. Some 44% are using Sharepoint.

Two thirds of respondents indicated that their TPRM program were in the earlier stages of maturity: initial, developing or defined.



41% are now locating their third party risk management program under a risk function. Procurement follows at 19%.

Most organizations are struggling to fully address the full life-cycle of third party relationships.

- Beyond third party risk - into fourth party and n-tier, there is still work to do. 20% of participants do not require third parties to disclose sub-contractors, 17% do not have controls in place for how third parties manage subcontractors, and 46% do not conduct due diligence on critical 4th parties.

- Of those that do manage these, most are doing so partially rather than fully. This is an area of risk exposure causing concern to the Regulators and it will serve companies well to embed more controls in this area.

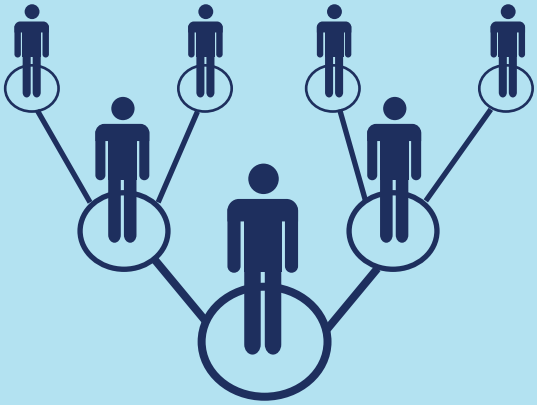
- TPRM teams worry about being able to keep up – with regulatory change, with the growing demands of an extended enterprise, and with the evolving nature of risk. This last point includes such hot button topics as cyber risk, data security, and concentration risk. While respondents were excited about the ability of TPRM to deliver real business value, they also recognize the importance of having the right infrastructure in place to support their TPRM program.

- Of all of the shortcomings of the current state of TPRM implementation, it is perhaps reporting that should cause the most concern. After all, it is through good reporting that TPRM will be able to communicate its value to key stakeholders such as senior management, the board, and regulators. Capturing the right information is the first challenge for firms – but being able to extract that information quickly and easily for analysis and decision-making is perhaps a bigger, second challenge. This is fundamental - not only will boards require accessible reporting for good governance but the lack of ability to quickly and comprehensively report will be a red flag to regulators.

  Contributing to this challenge will be:

  1) Lack of a single inventory
  2) Disparate systems across an organization
  3) Lack of integration between systems
  4) Technology limitations

Overall, there are good reasons in this survey to be optimistic about the future of this discipline. There is a clear pathway emerging: TPRM is beginning to consolidate around a clear set of best practices, even if organizations are taking longer to implement those practices than they would like. Budgets and salaries are not showing signs of general retrenchment, and those within the discipline are hopeful about their ability to deliver real value to their business.



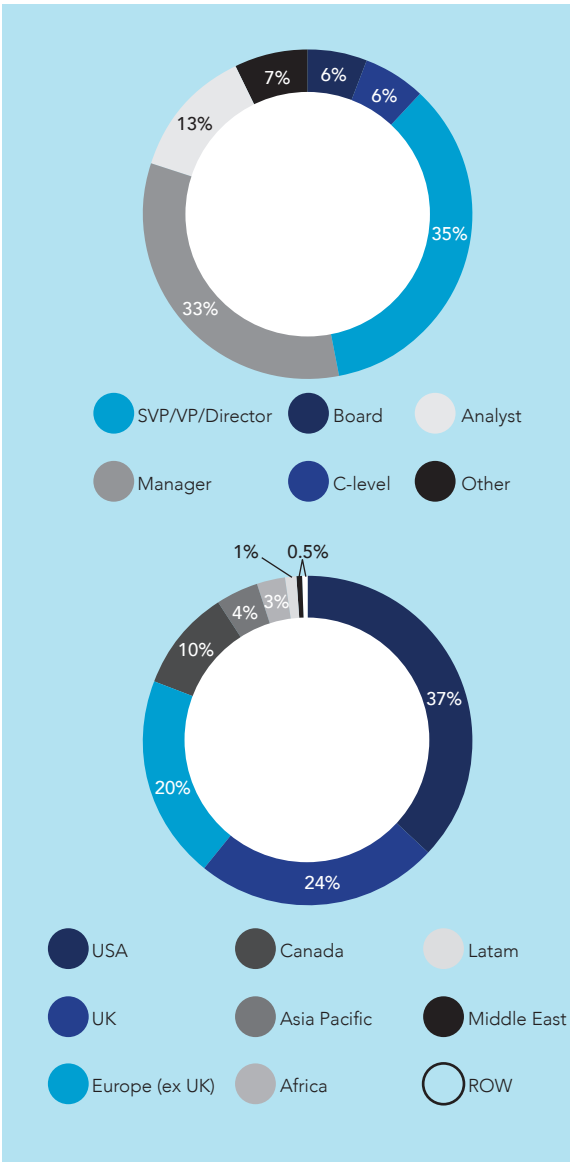
Fourth party risk is an area that TPRM now needs to address.

Reporting is a key challenge for TPRM - with the large majority of respondents unable to deliver standard reports quickly and completely

APPENDIX: DEMOGRAPHICS

What is your job level?

Overall, responses to the survey were from a relatively senior level of management within organizations. Slightly more than one-third of respondents were at the Senior Vice President (SVP), Vice President (VP) or Director level within their organizations. Another 12% were either from the C-suite or were sitting on the board of directors. One third of respondents were managers, while 13% were analysts within the TPRM discipline.

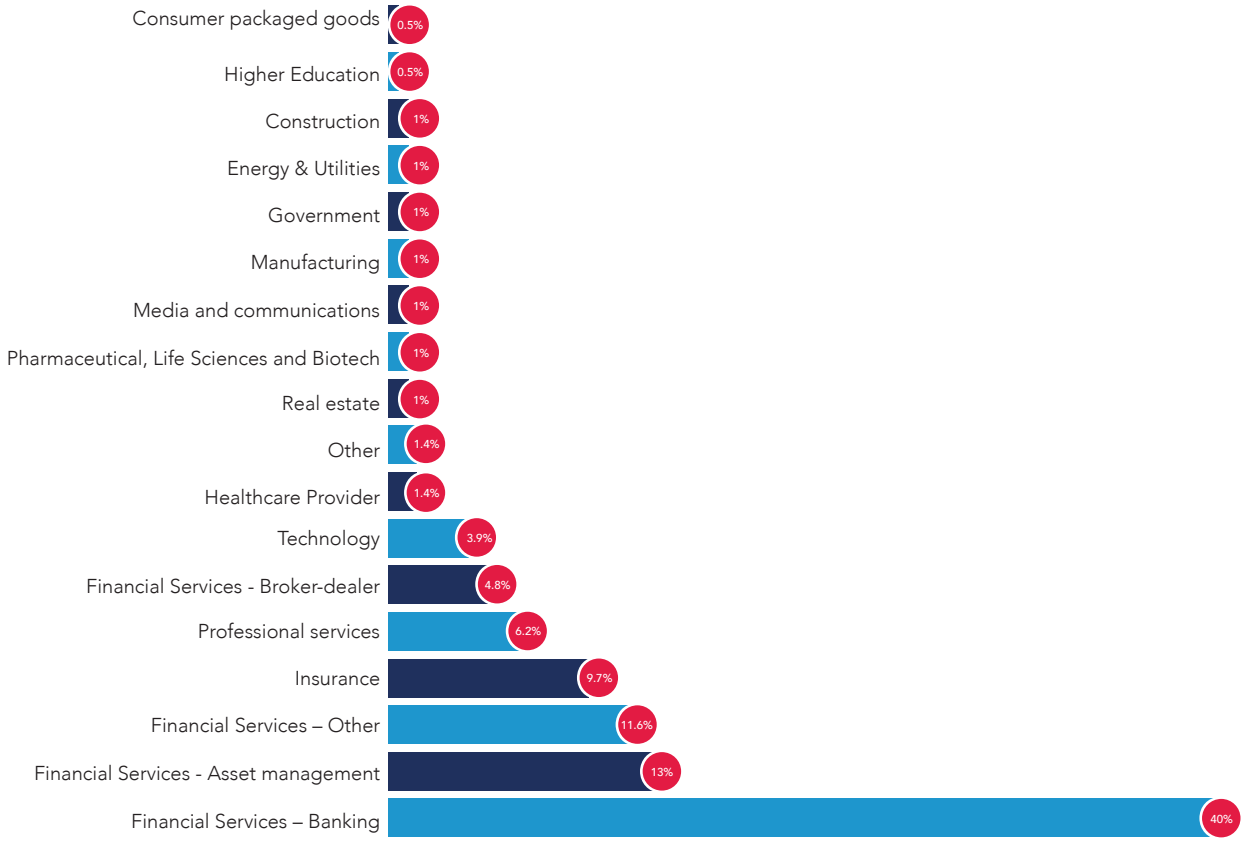


Where is your company headquartered?

The survey had responses from around the globe. Some 37% of responses were from US-based companies, with another 10% based in Canada. The United Kingdom was the location for the headquarters of 24%, while the rest of Europe was the home for 20% organizations.

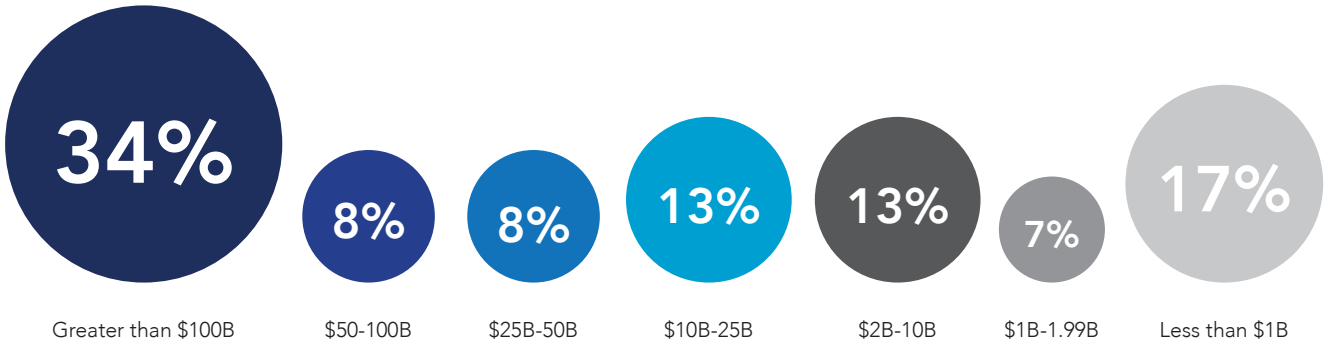
What best describes your industry?

The majority of responses for this survey hailed from the financial services industry – nearly eight out of 10. The non-financial services respondents hailed from a wide range of industries, including professional services (6.2%), technology, (3.9%) and healthcare (1.4%).



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

The respondents from the financial services industry came from institutes of a range of different sizes. While 34% had more than $100 billion in assets under management, 17% had less than $1 billion. Another 33% held assets between $1 billion and $10 billon, while 42% were in charge of assets between $10 billion and $100 billion.



Size of organization: Corporate by global revenue

Overall, the corporate respondents came from organizations that were a wide range of sizes. The largest group – nearly one-quarter – have between $5 billion and $30 billion in revenues. Some 12% have revenues of greater than $60 billion while 16% reported revenues of less than $100 million.