Third Party Risk Management outlook 2020

KPMG International

home.kpmg/thirdpartyrisk

Contents

Introduction

Organizations are increasingly reliant on third-party suppliers to deliver business-critical products and services to their clients and customers. They are also finding that failures by third parties can rapidly tarnish their reputations and have significant downstream operational and cost implications. As organizations address their concerns around these issues, it is evident that they need a clear strategy for the selection, approval and management of third parties. As there are a myriad of stakeholders involved, from the business as well as the procurement and risk oversight functions, developing and implementing this strategy continues to be highly challenging.

In simple terms, third-party risk management (TPRM) is the program that an organization uses to assess and manage its risks posed by third-party products and services. For example, with respect to a contract where an organization's data is being stored at the third party's premises, the organization needs to assess the risk of data security. A properly functioning TPRM program would involve the organization's Chief Information Security Officer — as manager of data security risk — in the Procurement process before contracting. In doing so, they can determine:

— How the third party will be accessing, storing or transmitting the organization's data

— Whether it has a control environment that meets the organization's expectations or needs to be enhanced

— If specific requirements should be negotiated into the contract.

Additional stakeholders from the risk function might include the Compliance department, which would determine whether or not the third-party service provider presents a risk of financial crimes or sanctions violations.

After the contract has been signed, the organization's TPRM program should focus on the ongoing management of the relationship, the performance of the third party, and the continued validation of the third party's compliance with control environment expectations.

Considering the importance attached to such activities, as well as the diversity of services being provided by third parties across most organizations, how can businesses ensure their TPRM program has the right governance structure, roles, and service delivery model? How can organizations balance the need to effectively manage risk across their third parties while also meeting the needs of relationship owners and other stakeholders within the business to engage third parties in a timely manner? Furthermore, how can the TPRM program best make use of innovation and new technologies to continuously assess the effectiveness of critical controls in an optimized approach?

It was with questions like these in mind that KPMG International embarked on a survey of 1,100 senior TPRM executives from major businesses across 14 countries and jurisdictions and multiple macro industry sectors worldwide.

In this report, we set out our key findings, recognizing that the principles of TPRM are broadly common across industries and geographies. To support organizations in their quest for TPRM program optimization, we also introduce key elements of our TPRM framework and methodology, which we have developed through extensive client experience.

As businesses adjust to new operating conditions, in the wake of the disruption caused by global events and economic uncertainty, many will reassess the risk profile of their third parties and re-evaluate their own resilience. As businesses do so, the need for a robust and sustainable TPRM program will be more important than ever before.

Defining third parties

Before we discuss our findings in detail, it is worth clarifying what we mean by certain terms used throughout this report. First, how do we define third parties?

Only a minority (41 percent) of respondents to our survey are fully confident that their business even has an agreed upon definition of 'third parties'. Within KPMG International and KPMG member firms, we include the following external parties within our definition of third parties: vendors, suppliers, service providers, agents, distributors, brokers, joint ventures, and resellers. Among internal third parties, we include affiliates, shared services, and parent companies/entities within the same group. We do not include customers within our definition, because businesses do not vet or onboard customers through a third-party program before entering into a transaction. Financial services firms, for example, onboard customers through a separate Know Your Customer (KYC) process.

Risks that are covered by a TPRM program

Secondly, when we talk about third-party risks, which specific risks are we referring to? In figure 1, we outline the main risk categories that all businesses are exposed to, as well as some of the individual threats that fall within these categories.

Depending on the nature of the third-party product or service being provided, each of these risks (and, more generally, a combination of several of them) may be present in the third-party relationship. TPRM programs should clarify roles and responsibilities for the identification and assessment of each risk type at the service or product level, so that requisite risk experts within the organization determine whether the third party can manage the risk in line with business expectations. There are, after all, many examples of companies being hit by severe penalties, as well as reputational damage, when a risk was not identified and mitigated, either via the third party's control environment or the company's internal compensating controls.

The #1 success factor for TPRM programs is the focusing of time, effort, and expertise on the highest-risk third-party services. In our survey, we found a mismatch between the risk areas that are considered mission critical for companies and the risks that are prioritized by the TPRM program. For example, our survey found that data

Figure 1. Potential risks for a TPRM program to cover

Regulatory/ compliance risk	— Regulatory requirements — Theft/crime/dispute risk	— Fraud, anti-bribery and corruption/sanctions — Compliance with internal procedures and standards
Strategic risk	— Service delivery risk — Expansion/roll-out risk — Mergers and acquisitions	— Alignment to outsourcing strategy — Intellectual property risk
Subcontractor risk	— Applicable across all risk areas	
Concentration risk	— Supplier concentration across critical services — Industry concentration (including subcontractor) — Concentration of critical skills (i.e. tech support)	— Geographic concentration — Reverse concentration
Technology/ cyber risk	— Information security — Cyber security — Data privacy/data protection	
Country risk	— Geopolitical risk — Climate sustainability	
Financial viability	— Financial risk from lending to a third party — Liquidity risk	
Operational/ supply chain risk	— Business continuity — Disaster recovery — Physical security — Operational resilience	— Performance management (including SLAs) — Model risk — Human resources risks (conduct risk, etc.)
Reputational risk	— Negative news — Lawsuits (past and pending) — Brand of the third party	— Key principals/owners of the third party — Workplace safety
Legal risk	— Jurisdiction of law — Terms and conditions of the contract	

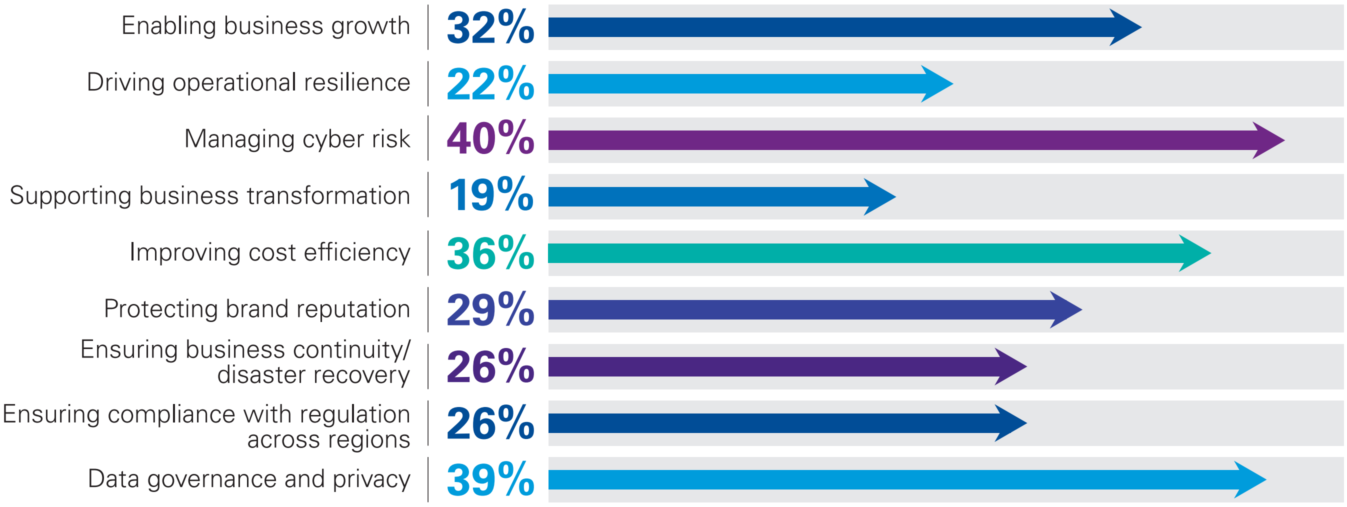
Source: Third Party Risk Management outlook 2020, KPMG International 2020

governance and privacy — along with cyber risk — is the most important driver of third-party activity across sectors and geographies (see figure 2). Nonetheless, when we examine the risks that businesses cover within their TPRM programs, in figure 3, just 54 percent of respondents prioritize data/privacy.

When speaking to David Hicks, Partner, KPMG in the UK, about this finding, he advised that "TPRM programs must have a well-defined and thought-through strategy, supported by a clearly articulated risk appetite. That way, programs have defined thresholds to manage against and report up to the board and senior management."

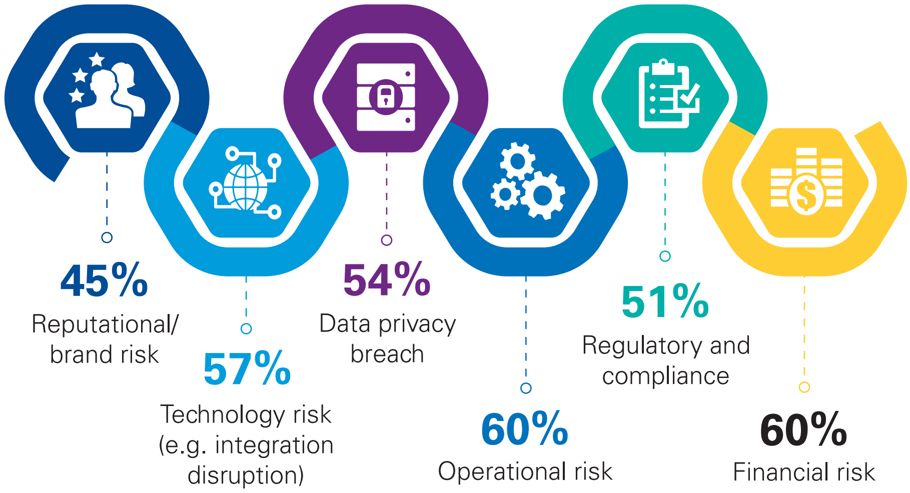
In re-examining this data, in the context of the new reality posed by global events and economic uncertainty, we have reflected on the low percentage (22 percent) attributed to Operational Resilience as a driver of TPRM activity. As Gavin Rosettenstein, Director, KPMG Australia, notes, "Recent discussions with clients have demonstrated that TPRM and Supply Chain teams are keenly invested in and cognizant of the role that third parties play in delivering critical business services to customers and clients. We expect operational resilience to continue motivating TPRM investment in years to come.

Figure 2. What are the most important drivers of TPRM activity in your business today?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Figure 3. Which of the following risks do you cover as part of your TPRM activity?



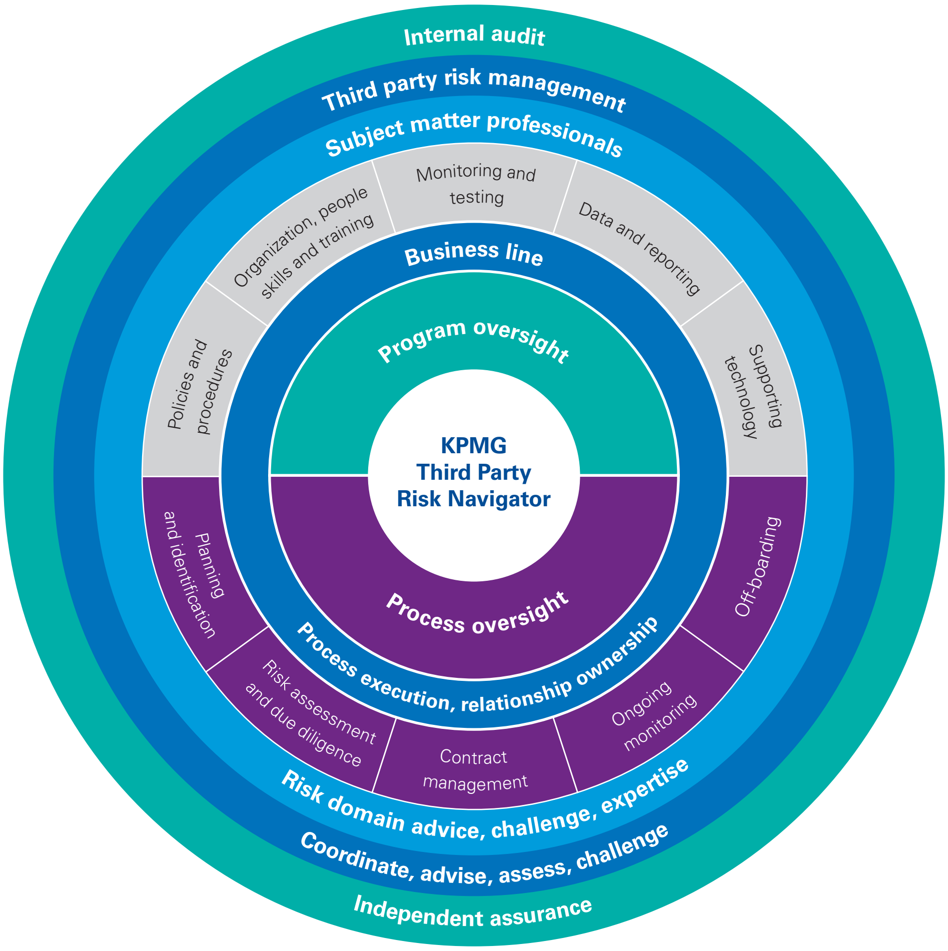
Source: Third Party Risk Management outlook 2020, KPMG International 2020

> "TPRM programs must have a well-defined and thought-through strategy, supported by a clearly articulated risk appetite. That way, programs have defined thresholds to manage against and report up to the board and senior management."
>
> — **David Hicks**
> Partner, KPMG in the UK

Distinguishing between the TPRM program and process

It is worth noting at the outset that we do not believe there is such a thing as a 'one-size-fits-all' TPRM program. That said, successful TPRM programs across industries do follow a defined process for identifying, monitoring, and managing third-party risk, under the leadership of defined program governance. Figure 4 outlines key areas of the TPRM program and how those areas apply to the end-to-end TPRM lifecycle.

Figure 4. Key areas of a TPRM program and end-to-end TPRM lifecycle



Internal audit
Third party risk management
Subject matter professionals
Monitoring and testing
Data and reporting
Supporting technology
Organization, people skills and training
Policies and procedures
Business line
Program oversight
KPMG Third Party Risk Navigator
Process oversight
Planning and identification
Off-boarding
Process execution, relationship ownership
Risk assessment and due diligence
Contract management
Ongoing monitoring
Risk domain advice, challenge, expertise
Coordinate, advise, assess, challenge
Independent assurance

Source: Third Party Risk Management outlook 2020, KPMG International 2020

In the next section, we discuss our key findings from the survey. In section 2, we outline KPMG's purpose-built framework for building an effective TPRM operating model. Finally, in section 3, we set out the steps that businesses should take in order to drive positive change and realize maturity.

We hope you find this overview useful and would be happy to talk it through with you in more depth.

> "Recent discussions with clients have demonstrated that TPRM and Supply Chain teams are keenly invested in and cognizant of the role that third parties play in delivering critical business services to customers and clients."
>
> — **Gavin Rosettenstein,** Director, KPMG Australia

Section 1:

Key findings of our survey

TPRM is a strategic priority

More than three out of four respondents to our survey (77 percent) say TPRM is a strategic priority for their business. Additionally, six out of 10 respondents say their organization's most severe reputational risks come from its third parties' failure to deliver. These findings highlight how dependent most businesses are on third parties to deliver critical products and services to their clients and customers. At the same time, growing regulatory pressure — particularly in relation to privacy breaches and the loss of customer data, or to Operational Resilience — is putting third-party relationships under additional scrutiny. Six out of 10 (59 percent) respondents stated that their organizations had recently been subject to sanctions and regulatory findings in relation to TPRM.

Global events and economic uncertainty underlined how necessary third parties are for business operations. KPMG has defined four phases for businesses to consider in the wake of a pandemic or global event and economic uncertainty: Reaction, Resilience, Recovery, and the New Reality. Specifically, with respect to TPRM, the first two of these phases deal with the emergency shift to remote-working models and the reconfiguration of third-party service delivery models to ensure services are being maintained for clients and customers. The second two phases cover preparation for how businesses will operate in the New Reality, where control environments are distributed further to homes for remote contingent workers and where social distancing is required at work locations to prevent subsequent virus breakouts. TPRM programs will also have to consider what new government regulations may arise, and updates to the TPRM program may be necessary due to the general uncertainty around the resilience of the third-party ecosystem as the financial impacts of the crisis manifest.

Companies are inconsistent in their approach to TPRM

Businesses work with a wide variety of third parties worldwide, and each third party manages a subset of risks on the business's behalf. For good reason, businesses need to understand each third party's ability to manage risks in line with expectations before deciding whether to engage that third party. Worryingly, however, our research suggests that many organizations are not prepared for the complexity that comes with assessing multiple risks in a cohesive manner across business lines and regions. Holistic risk identification and assessment upfront in the onboarding process, as well as during the lifecycle of the contract, is crucial for organizations to have line of sight into the risk profile of their entire third-party portfolio. Three-quarters (74 percent) of respondents admit that their organizations urgently need to make TPRM more consistent across the enterprise.

A risk-based approach is the number 1 'get right' for TPRM programs

Managing third-party risk in today's business environment is far from straightforward, and the scope of the program, along with the amount of coordination involved, causes some to feel overwhelmed. The situation is not helped by limitations in organizational resources and budget. Half of businesses do not have sufficient capabilities in-house to manage all the third-party risks they face. In our view, organizations can achieve both efficiency and

effectiveness by taking a risk-based approach to assessing and monitoring third-party products and services that present the highest risk to the organization.

Data and technology are improving TPRM teams' performance

Across industries and regions, respondents indicated that the sheer volume of third-party assessment activities has increased in recent years. At first, TPRM programs simply increased their headcount to complete a greater number of risk assessments. Today, organizations have the potential to innovate their approach in three areas:

— Greater automation of the TPRM process internal workflow

— Leveraging shared utility providers for due diligence questionnaires and responses

— Moving away from point-in-time risk assessments to continuous controls monitoring.

At present, we only see about a quarter of businesses using technologies to improve either the workflow automation or monitoring of third parties. Technology is, however, the most favored investment (61 percent) that respondents make when additional funding is made available to them.

"It is an exciting time to be working in TPRM, "says Jon Dowie, Partner, KPMG in the UK, "since the industry has finally reached a consensus that our approach to point-in-time risk assessments needs to evolve. Companies across industries are collaborating on common standards for questionnaires and shared assessments, so that their teams can focus on treating third-party risks, rather than chasing down questionnaire responses or traveling for on-site assessments."

It's time to sustainably scale the program

Organizations are maturing their TPRM programs to better understand where they are at risk of service disruptions resulting from third-party non-performance. Further, organizations are expanding risk identification, assessment, and management to material subcontractors. As we explore in the next section of this report, many organizations have room for improvement across their entire operating model, inclusive of governance, process, infrastructure, and data. With that in mind, our analysis has helped us refine the steps that organizations should take to upgrade their TPRM programs. These steps — which we outline in section 3 of this report — focus on helping teams uplift their programs, optimize processes, and take advantage of new technologies to achieve better results with the limited resources available.

> "Companies across industries are collaborating on common standards for questionnaires and shared assessments, so that their teams can focus on treating third-party risks, rather than chasing down questionnaire responses or traveling for on-site assessments."
>
> **— Jon Dowie**
> Partner, KPMG in the UK

Section 2:

A framework for effective TPRM

Greg Matthews, Partner, KPMG in the US says, leading TPRM programs are experimenting with new operating models to identify, monitor, and manage third-party risks more efficiently — without compromising on effectiveness. “Achieving TPRM transformation will require programs to overcome the roadblocks that have plagued these programs throughout their initial build and subsequent iterations, such as inadequate executive support, insufficient accountability, and resistance from third parties to cooperate with the TPRM process,” he explains.

KPMG’s framework for an effective TPRM operating model is based around four pillars: governance, process, infrastructure, and data. Each of these pillars has specific requirements, which we set out below. One point of concern is that many companies still have a long way to go before they reach maturity, as illustrated by data from our survey.

> “Achieving TPRM transformation will require programs to overcome the roadblocks that have plagued these programs throughout their initial build and subsequent iterations.”
>
> — **Greg Matthews**
> Partner, KPMG in the US

Governance

What is required?

— A single leader of the program

— A reporting structure to senior management and the Board

— An outsourcing and third-party strategy for the organization, as well as a defined risk appetite

— Clear roles, responsibilities, and accountabilities across the TPRM program and the end-to-end TPRM lifecycle

— Policies, standards, and a risk appetite that establish the scope and focus of the program

— An inventory of third-party services to which the program applies, based on agreed-upon definitions of third-party services.

Why businesses need to take action:

— 74 percent of respondents say their organization urgently needs to make TPRM more consistent across the enterprise

— 57 percent of respondents say their organization is a long way from having an enterprise-wide agreement for services that can and cannot be outsourced.

Process

What is required?

— Consistency of execution across the TPRM program to drive quality data for analysis

— Assessment teams that have the right mix of skills, expertise, and bandwidth

— A risk-based approach to assessing third-party services that is tied to the program’s risk appetite

— A risk assessment that takes place prior to contract execution and supporting decision-making

- Continued risk analysis and mitigation, rather than a myopic focus on data collection and questionnaire-response gathering
- Ongoing monitoring over the lifetime of contracts, inclusive of continuous monitoring
- Procedures and templates that clarify processes and drive consistency
- Coverage of fourth-party and material subcontractor risk, in addition to third parties.

Why businesses need to take action:

- 52 percent of respondents believe their organization's TPRM program is over-engineered and impedes their ability to do business
- Skills shortages are respondents' number one challenge when trying to transform their TPRM activity
- 67 percent of respondents say that their organization's third-party risk assessments are carried out by numerous resources across the organization, rather than by one person or team
- Just 32 percent of respondents say that their organizations are highly proficient at developing a comprehensive understanding of the risks posed by a third party
- Just 36 percent of respondents say that their organizations have a risk-based approach to ongoing monitoring
- 40 percent of respondents say that their organizations don't carry out monitoring of third parties after contracting, often because they allowed this monitoring activity to lapse over time
- 72 percent of respondents say that their organizations urgently need to improve how they assess fourth parties.

Infrastructure

What is required?

- A TPRM technology architecture that supports efficient workflow, task automation, and reporting
- A documented and well understood audit trail
- A service delivery model that is aligned to the company's operating style (either centralized or distributed) and allows for consistent management of risk across business lines and regions
- The integration of TPRM activities and technology into existing firm-wide processes, such as Procurement, Legal, and Finance, and into existing risk oversight functions and activities.

Why businesses need to take action:

- There is little consistency, across businesses, on which operating model to use, with ultimate responsibility for TPRM differing noticeably across businesses (see figure 5)
- Just 24 percent of respondents say that their organizations are using automation to enhance efficiency in the TPRM program by carrying out routine tasks.

Data

What is required?

- The collection of real-time data around the TPRM program's ability to manage the company's third-party assessment, onboarding, and monitoring activities and its ability to manage the specific performance of each third-party service and the control environments in which they operate
- A comprehensive data model for the collection of third-party information, including service details, risk scoring, contract information, and performance monitoring
- Internal data feeds that monitor for and record specific events and incidents that are attributable to third parties, and external data feeds that monitor for real-time information on the third parties, such as adverse media, changes in business ownership, corporate actions, cyber vulnerability scores, and financial viability ratings
- A process to update third parties' risk profiles when there are changes to the risk score, ideally in real time as issues or external drivers arise or as there are changes to the third party's control environment
- Real-time tracking of performance against service level agreements (SLAs)
- Real-time tracking of risks against key risk indicators (KRIs)
- Data-driven decision making, where risk assessments and performance monitoring influence contract terms and decision-making during re-contracting or the continuation of the third-party relationship.

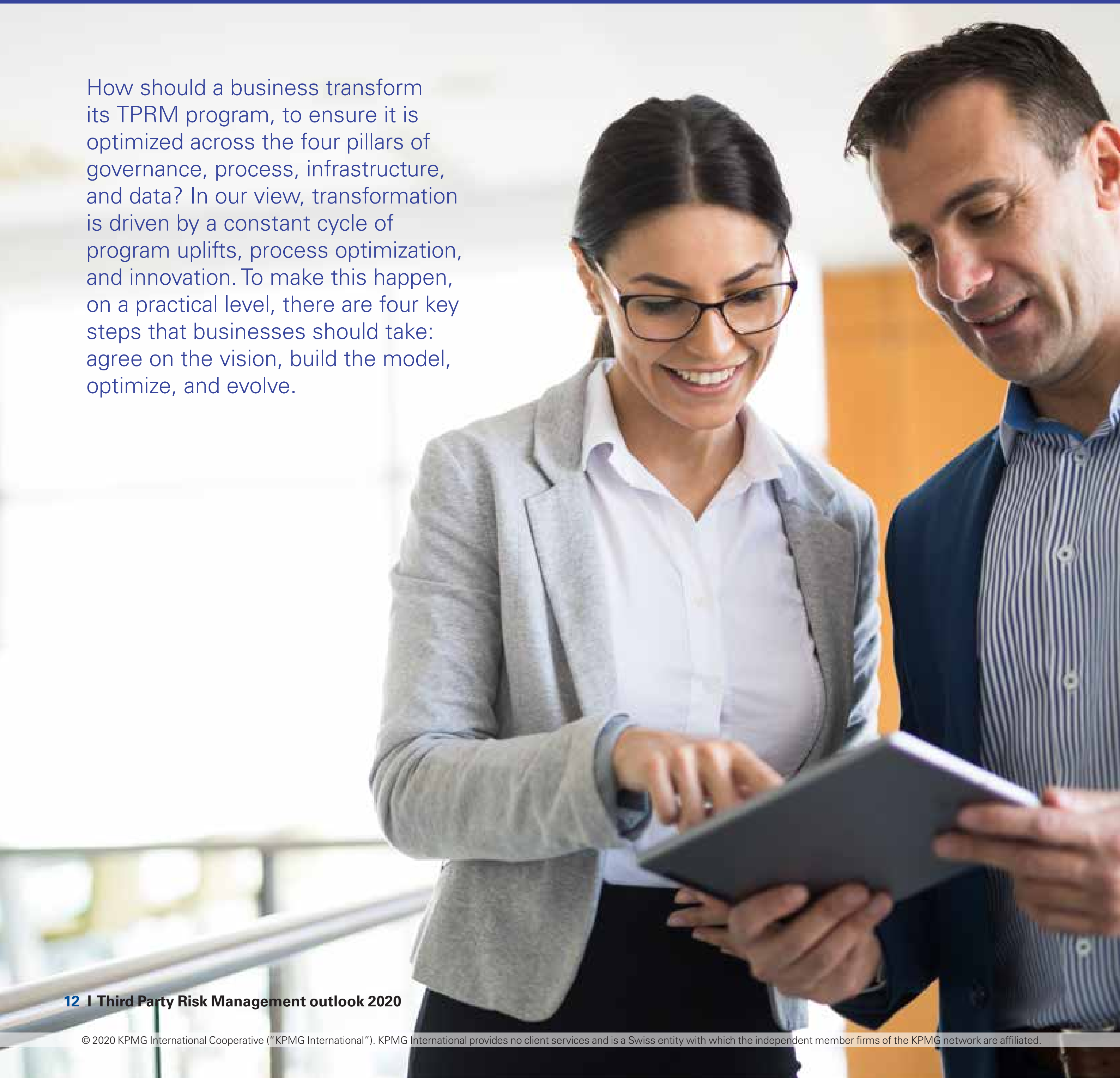
Why businesses need to take action:

- 37 percent of respondents say technical barriers, such as incompatible systems, are their organization's main barrier to sharing third-party data across the enterprise
- Less than half of respondents are very confident in their organization's electronic inventories of third-party contracts, risk monitoring and reporting, and inventories of third parties
- Just one in four (26 percent) respondents believes strongly that their organization has all the data needed to carry out assessments.

Section 3:

Journey to TPRM maturity

How should a business transform its TPRM program, to ensure it is optimized across the four pillars of governance, process, infrastructure, and data? In our view, transformation is driven by a constant cycle of program uplifts, process optimization, and innovation. To make this happen, on a practical level, there are four key steps that businesses should take: agree on the vision, build the model, optimize, and evolve.



1 Agree on the vision

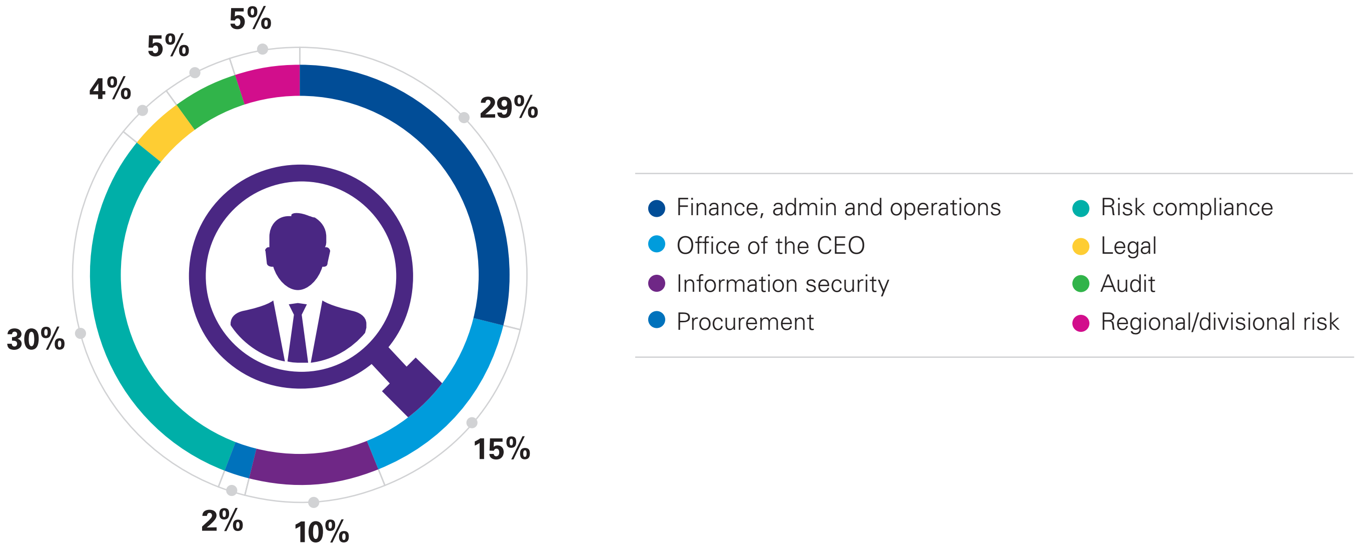
Almost all businesses have some form of TPRM program in place. Although 51 percent of respondents' organizations are working with limited budgets, given the increased focus on the use of third parties, three in four (76 percent) respondents indicate that funding is available or growing to evolve and strengthen their organization's TPRM program.

A key consideration for the enterprise-wide TPRM program is designating program ownership and determining where TPRM sits within the organization. This is ultimately decided by the nature and complexity of each business, though our research found that responsibility is most likely to fall under Risk and Compliance (30 percent) or Finance, Admin and Operations (31 percent) — see figure 5. Within the latter group, organizations are increasingly identifying the Procurement function to execute the TPRM lifecycle activities.

"We find that placing TPRM within the broader procurement organization can lead to significant operational efficiencies and an improved user experience for business relationship owners of third-party services," says Alexander Geschonneck, Partner, KPMG in Germany. "That said, there may be a skillset uplift and cultural change required to prepare the procurement function to take on the execution of TPRM, as well as potential reporting line complications for third-party risk reporting to risk committees and the Board."

> “We find that placing TPRM within the broader procurement organization can lead to significant operational efficiencies and an improved user experience for business relationship owners of third-party services.”
>
> — **Alexander Geschonneck,** Partner, KPMG in Germany

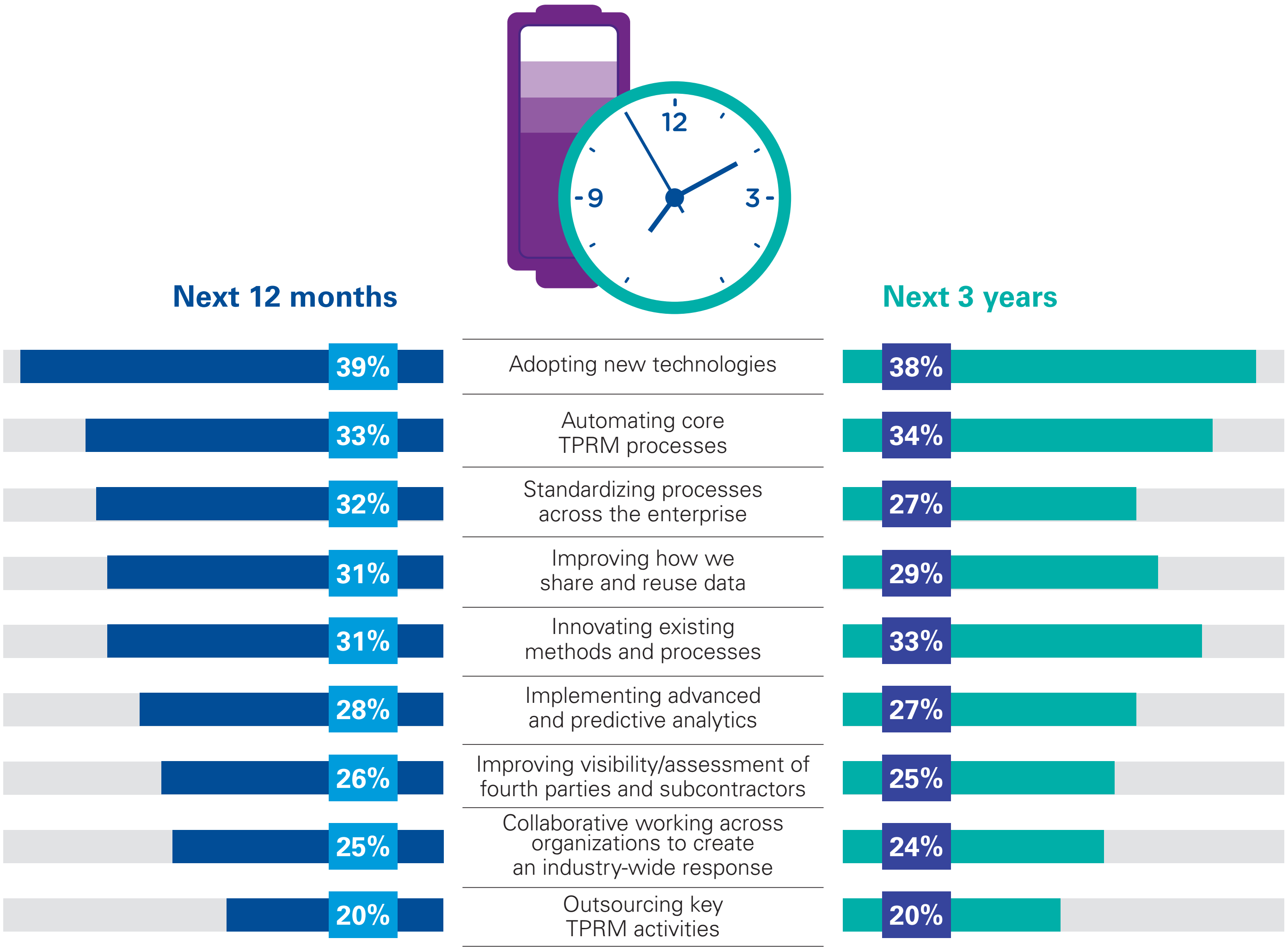
Figure 5. Who is ultimately responsible for TPRM in your business?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Second to establishing program vision, guardrails, and ownership is determining the aspirations for technology enablement. In this respect, businesses should be careful to not attempt to 'run before they walk.' While many organizations recognize that automation of the program as a whole is essential for scaling TPRM and for helping teams to process and analyze large volumes of data — as illustrated by figure 6 — technology should be seen as an enabler rather than the driver of progress. Automating weak processes will not magically enhance those processes.

Figure 6. On which of the following initiatives will your team be focusing the most time and energy over the next 12 months, and next 3 years?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

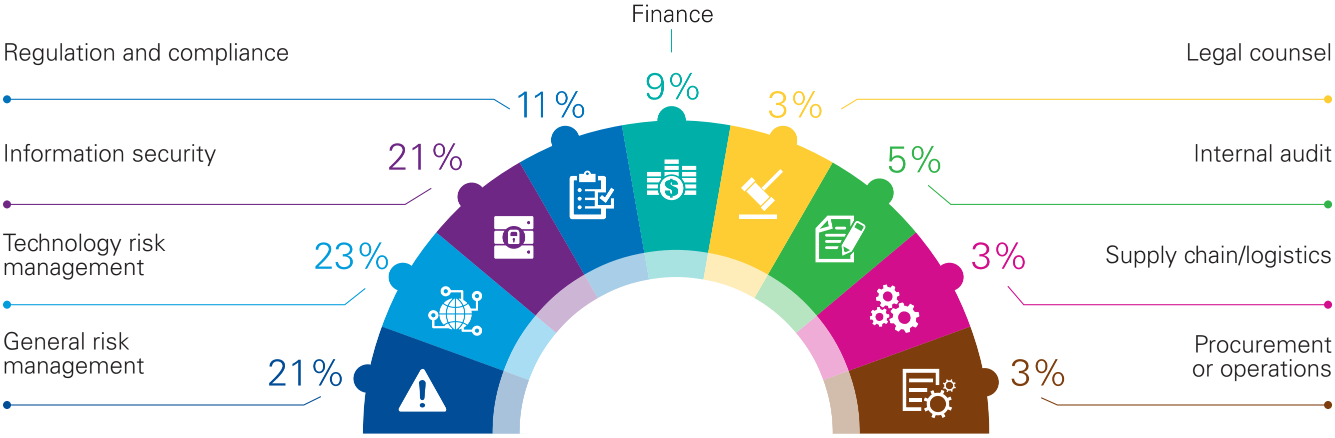
2 Build the model

TPRM programs are complex. Not only does every part of the organization use third parties, each third-party service has multiple risks, and different oversight functions need to be consulted on individual risk assessments. As Amanda Rigby, Partner, KPMG in the US, explains, "After the program is established, businesses continue to tweak and clarify how it works as they enhance its effectiveness across the enterprise. TPRM program development is not a one-time exercise. Most clients have gone through three or more iterations of the program before they strike the right balance for their organization."

Considerations at the program building stage include deciding exactly how, when, and where to involve business stakeholders throughout the TPRM lifecycle. Procurement, for example, generally owns the onboarding and third-party management process, while business owners and centralized TPRM assessors interface with the risk subject matter experts at critical points, such as during the initial and ongoing risk assessment process (see figure 7 for a summary of the main groups involved). Beyond this, the TPRM program team is largely charged with executing the program; the risk-oversight functions are responsible for the risks they oversee; and the business is accountable for the management of the third-party service on a day-to-day basis.

> TPRM program development is not a one-time exercise. Most of our global clients have gone through three or more iterations of the program before they strike the right balance for their organization.
>
> — **Amanda Rigby,** Partner, KPMG in the US

Figure 7. Who provides second line of defense for TPRM?



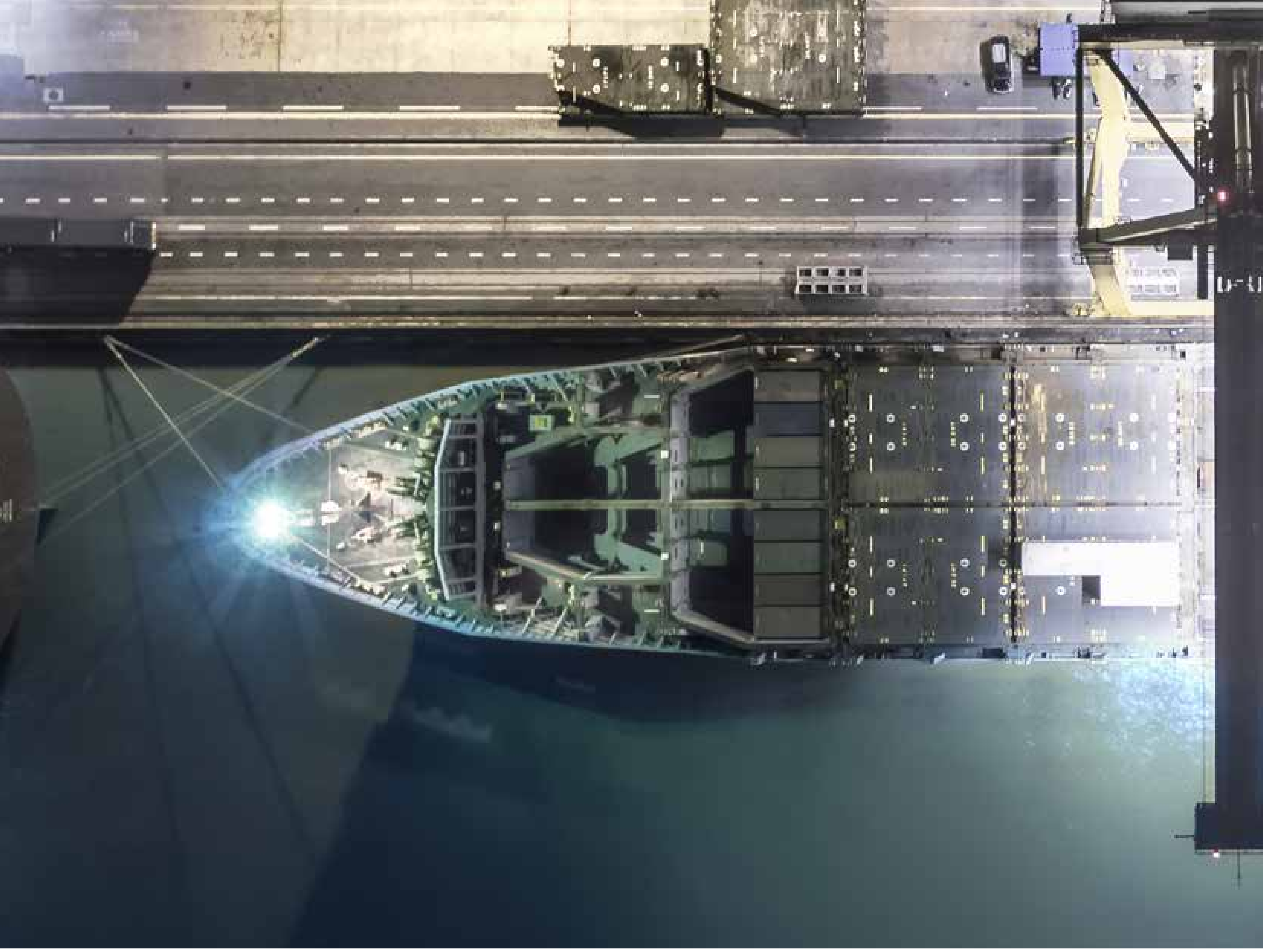
Source: Third Party Risk Management outlook 2020, KPMG International 2020

Another consideration is around which model to use for completing risk assessment activities. Businesses may opt to use a distributed model, through which the business relationship manager coordinates inherent risk assessment activities. Alternately, businesses may identify a centralized team that facilitates the inherent risk assessment on behalf of (and with input from) the business. In this model, the centralized team helps business relationship owners overcome challenges around integration and skills shortages and drives a higher degree of consistency, which is key because inherent risk information is the foundation of TPRM program analytics.

"In many cases, we see that there is an overall higher cost to maintain a distributed model because of the training and oversight required across the vendor managers," says Lem Chin Kok, Partner at KPMG in Singapore. "We see hybrids of the two models, but most often there is a greater leaning toward a centralized model than there is toward a distributed model, where the centralized team executes the risk assessment activities and provides the outputs to the business relationship managers, who finalize the decision to proceed with the third-party provider."

Often times, organizations have specific requirements that have to be built out in parallel; for example, in today's climate, multinational organizations also have to ensure they are addressing growing global regulatory requirements and nuances across regions. Getting the right support from Compliance and Technology Risk Management is essential when it comes to refreshing the program on an ongoing basis to comply with requirements and keep pace with new regulatory expectations, including customer and client data privacy.

Another area of focus for survey respondents is fourth-party and material subcontractor risk management. An example of a material subcontractor relationship is one in which the third party uses a cloud provider to support the delivery of its service. Businesses need to establish consistent oversight of these fourth parties, which is no small feat, given there is no direct contract between the organization and its fourth parties. When it comes to fourth-party risk management, organizations generally employ one or more of the measures outlined in figure 8. Understanding the role of the subcontractor within the delivery of the third-party service, including data the



fourth party has access to and how its role influences business continuity risks, is vital to gaining a complete risk picture of the service the organization is entering into. Understanding whether the third party has a program in place to manage its third parties (i.e. the organization's fourth party) is an important part of the assessment of whether or not to allow the third party to use subcontractors.

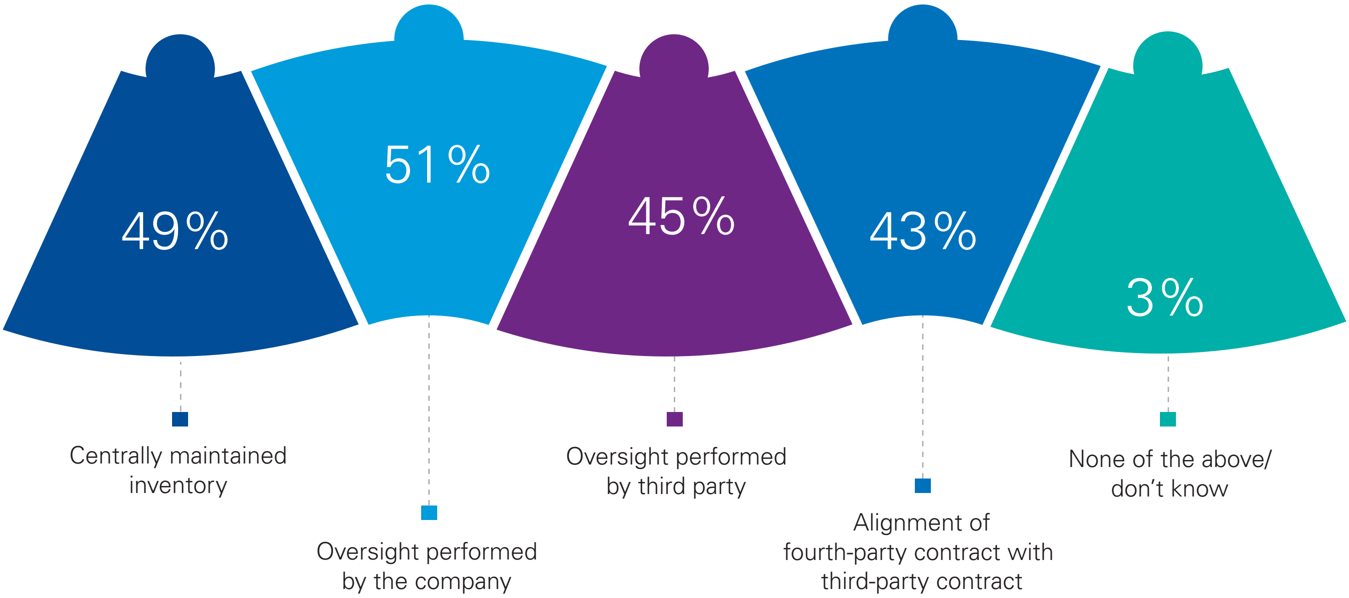
> “We see hybrids of the two models, but most often there is a greater leaning toward a centralized model than there is toward a distributed model.”
>
> — **Lem Chin Kok**
> Partner,
> KPMG in Singapore

Resolving these initial considerations is a major step forward but is only part of what is required before full TPRM program maturity can be attained. Organizations need to expand their TPRM programs to take into account not only the pre-contract risk assessment but also ongoing monitoring across the life of the contract.

3 Optimize the process

Process optimization aims to ensure that third parties that do not meet pre-determined risk criteria and materiality thresholds are not put forward for assessment by the TPRM program. Organizations can optimize the risk stratification process in two ways: risk segmentation — establishing a disciplined risk-scoring methodology across third-party services — and enhancement of the service delivery model to reduce costs and increase accountability. These actions will help address the organizational budget limitations that were flagged by respondents to our survey, as well as support teams in making the right decisions with the data available to them.

Figure 8. Which of the following processes and practices do you have to manage fourth-party risk?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Organizations should segment third parties into three categories:

- those which present nominal risk to the organization and do not need to be risk assessed
- third parties that are appropriate for the standard TPRM process
- third parties that present a homogenous risk profile and are more efficiently managed centrally, via a specialty program.

With respect to risk segmentation, the aim should be to enable customization and tailoring for third parties that do not present the standard risk profile for third-party risk assessment requirements. For example, a third party from which the organization purchases office supplies may not warrant the same degree of assessment as a third party to whom the organization is outsourcing a core customer contact center.

Practically, this is achieved through aligning the Procurement service categories with nominal risk or specialty program designations. For the standard TPRM process, the first step is to ask a series of gating questions upfront, including:

- Does the third party interact with our clients/customers?
- Is the work performed in the same country as the organization?
- Will the third party have access to intellectual property or customer/client data? If so, will the data be stored in the cloud?
- Is the third-party service related to an area of regulatory scrutiny or requirements?
- Does this third-party service represent a material outsourcing or critical function?

An affirmative response to any of the above questions may drive the involvement of the associated risk oversight function and the completion of the specific risk questionnaires and due diligence assessments. On the other hand, negative responses to these questions may limit the volume of risk assessment activities, decreasing effort and costs.

When it comes to optimizing the TPRM service delivery model, we see leading programs carrying out a review of who in the organization should complete TPRM activities. The biggest challenge of a distributed model, where the third-party relationship manager is heavily involved, is lack of skills. During global events and economic uncertainty, some organizations were also challenged in getting accurate, updated information about third-party services, acknowledging that third-party relationship managers were already under increased pressure.

Likely in response to such talent challenges, respondents indicate that training and skills development is a key focus area for their organization's TPRM programs (see figure 9). Recognizing that risk domain expertise is limited across organizations, many clients are centralizing aspects of TPRM process execution and determining where a generalist may be able to complete aspects of the risk assessment and due diligence processes. Organizations are determining which controls and risk areas require the dedicated focus of a domain expert. While a centralized team may execute risk assessments and scoring, the business is still accountable for making the decision to proceed (or not) with contracting the third party. Our view is that clearly defining these structural components of the TPRM process allows organizations to automate tasks, structure workflows, and simplify the collection and analysis of information by different teams.

4 Evolve and innovate

Given that the greatest effort in the TPRM program revolves around the gathering of information and assessment of third-party control information, these are the areas where we see the greatest focus on investment. In the coming years, we anticipate significant progress across two broad topics:

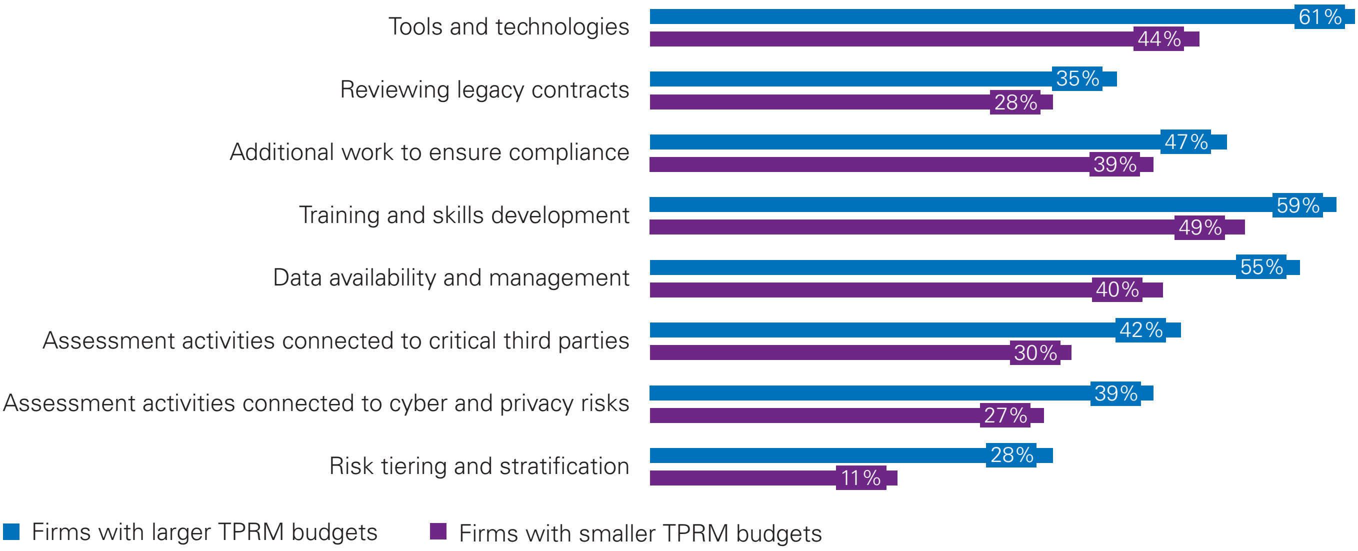
- The sharing of due diligence responses across the industry
- The use of technology and scoring services to assess third-party control environments in a more continuous and consistent manner.

The majority of survey respondents are leveraging or looking to leverage shared assessment information to reduce costs. There is an increasing acknowledgement and acceptance that industry utilities may collect and share information between third parties and their customers. The value proposition is clear for third parties and their customers. For third parties, the collection and sharing of information might mean that a utility collects the information once, completes the assessment once, and then offers assessment results to all of its customers, rather than having each customer conduct a separate risk assessment. In this scenario, the value proposition for customers would come from receiving necessary assessment information in a timely manner and sharing the associated risk-assessment costs across the industry.

With respect to TPRM technology innovation, our survey indicates that businesses are focusing their limited budgets on new tools (see figure 9). This is in line with our experience, based on the maturity of TPRM programs. In the past, organizations accomplished an increased volume of assessment activities by increasing headcount. Now, we see leading TPRM teams using automation, data analytics, and natural language processing, as well as incorporating scoring services for affordable and scalable continuous monitoring across select risk areas, performance management, and contract compliance. TPRM programs are exploring how they can use machine learning to evaluate internal data around risk events and identify those risk events that may have been caused by a third party. They are automating the monitoring of their third parties' compliance with SLA terms, identifying opportunities to recoup fees for missed commitments, and taking a more proactive approach to reputational risk, such as by automating analysis of social media data.

Some of these innovations are growing in attractiveness as teams adjust their programs to address the challenges presented by global events and economic uncertainty and its aftermath. Given the current limited ability of organizations to conduct on-site reviews, organizations are identifying ways to update the TPRM program to address the new reality, such as determining how continuous monitoring can accomplish certain goals of the TPRM program in lieu of the standard risk questionnaire, due diligence assessment, and on-site review. Organizations are also rethinking how data-driven, proactive risk monitoring — leveraging AI and machine learning — can identify early-warning indicators for third-party resilience and can help mitigate the impact of future crises. Finally, organizations are considering how to more accurately price in the risk of pandemics and other tail risks.

Figure 9. Where are you investing your funds for TPRM?

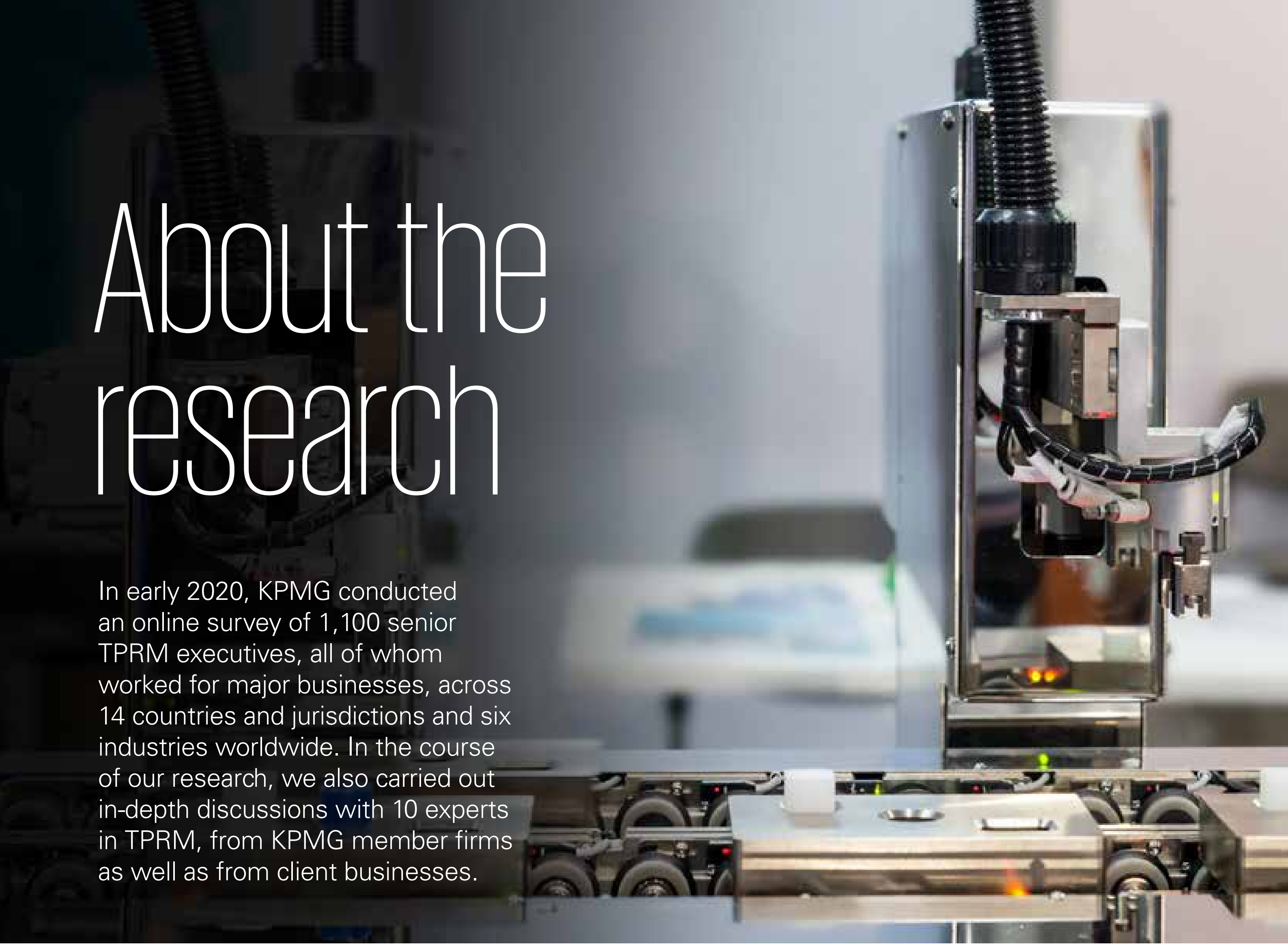


Source: Third Party Risk Management outlook 2020, KPMG International 2020

Conclusion

Our research confirms that organizations across all sectors and geographies are rightfully considering TPRM to be a strategic priority. We see businesses taking a proactive approach to TPRM and exploring how they can refine and expand their existing processes through technology enablement and innovation.

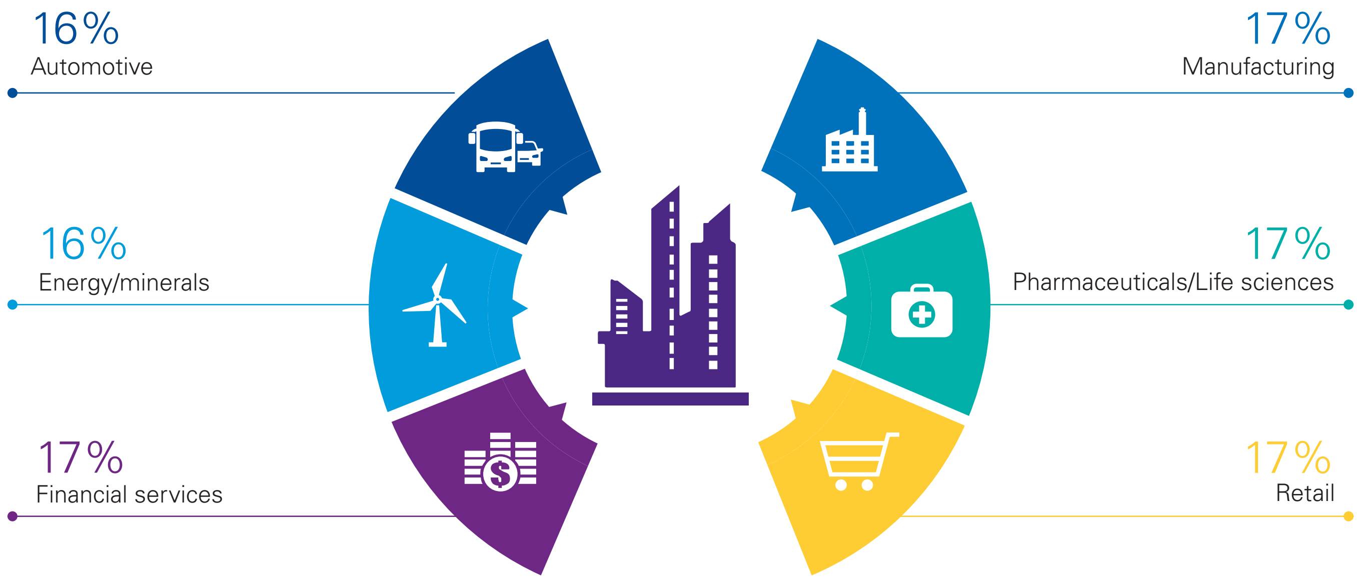
That said, our survey also makes clear that, for many organizations, TPRM remains a work in progress. As they adjust to global events and economic uncertainty, organizations may also find that their historical third-party assessment information and control environment analysis needs to be updated to account for new risks and challenges. As a matter of the utmost urgency, organizations should improve the business resilience across critical customer/client services by accurately understanding the role third-parties play in delivering these services and adjusting policies and controls accordingly.



About the research

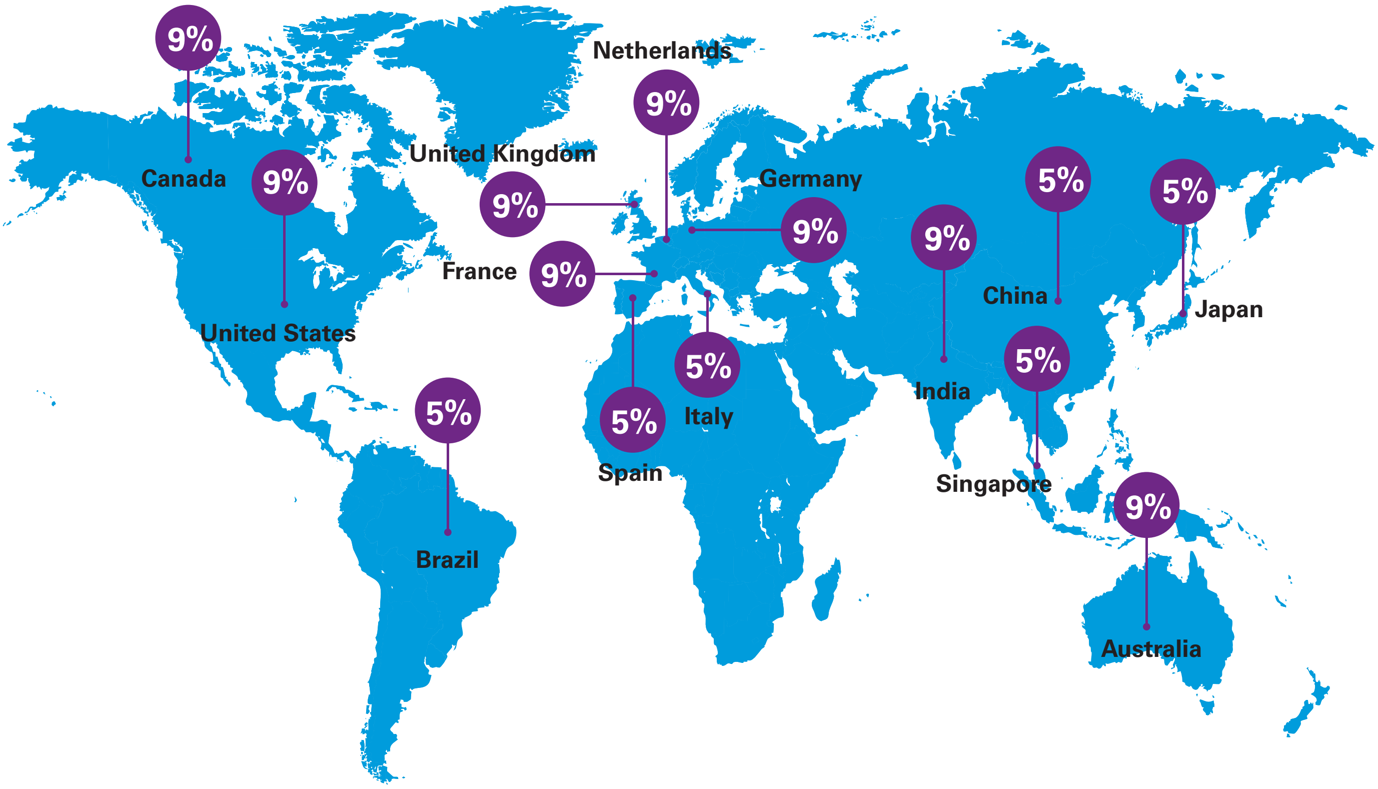
In early 2020, KPMG conducted an online survey of 1,100 senior TPRM executives, all of whom worked for major businesses, across 14 countries and jurisdictions and six industries worldwide. In the course of our research, we also carried out in-depth discussions with 10 experts in TPRM, from KPMG member firms as well as from client businesses.

Figure 10. In which sector does your company operate?



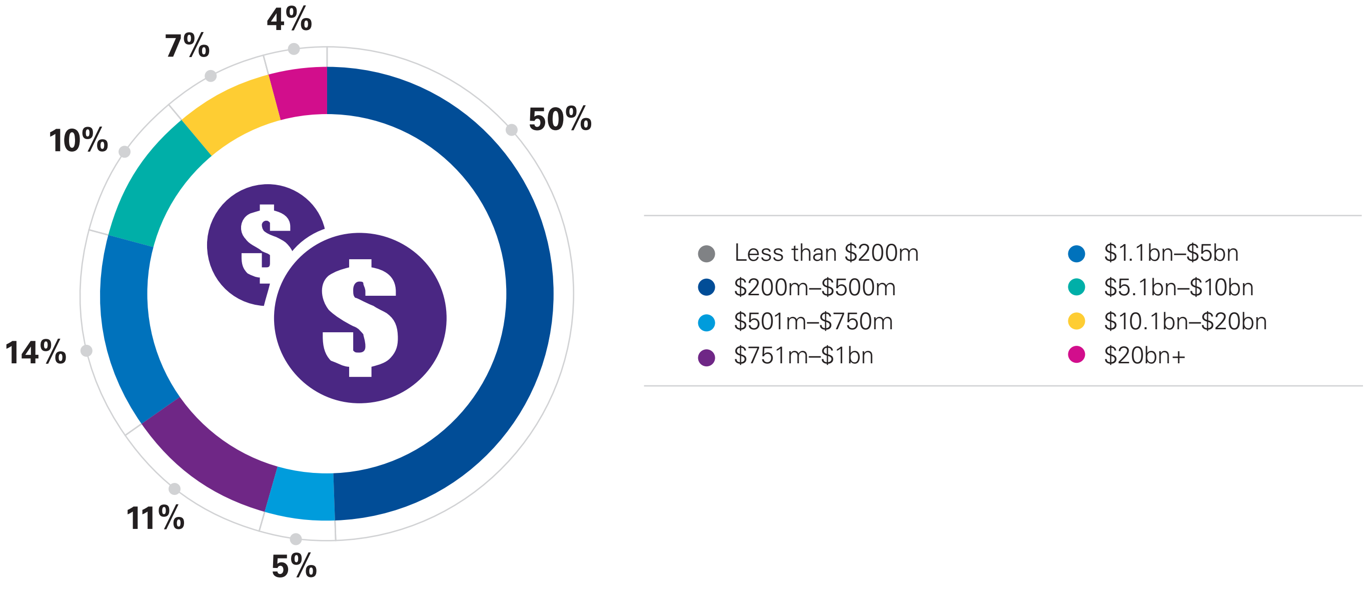
Source: Third Party Risk Management outlook 2020, KPMG International 2020

Figure 11. In which country/jurisdiction does your company primarily operate?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Figure 12. What is your organization's total global annual revenue in US$?



Source: Third Party Risk Management outlook 2020, KPMG International 2020

Contacts

David Hicks
Global Forensic Leader
KPMG International
T: +44 207 6942915
E: david.hicks@kpmg.co.uk

Alexander Geschonneck
Partner
KPMG in Germany
T: +49 30 2068 1520
E: ageschonneck@kpmg.com

Greg Matthews
Partner
KPMG in the US
T: +1 212 954 7784
E: gmatthews1@kpmg.com

Lem Chin Kok
Partner
KPMG in Singapore
T: +6562132495
E: clem@kpmg.com.sg

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg

home.kpmg/socialmedia

Throughout this document, "we", "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by Evalueserve.

Publication name: Third Party Risk Management outlook 2020

Publication number: 137087-G

Publication date: July 2020