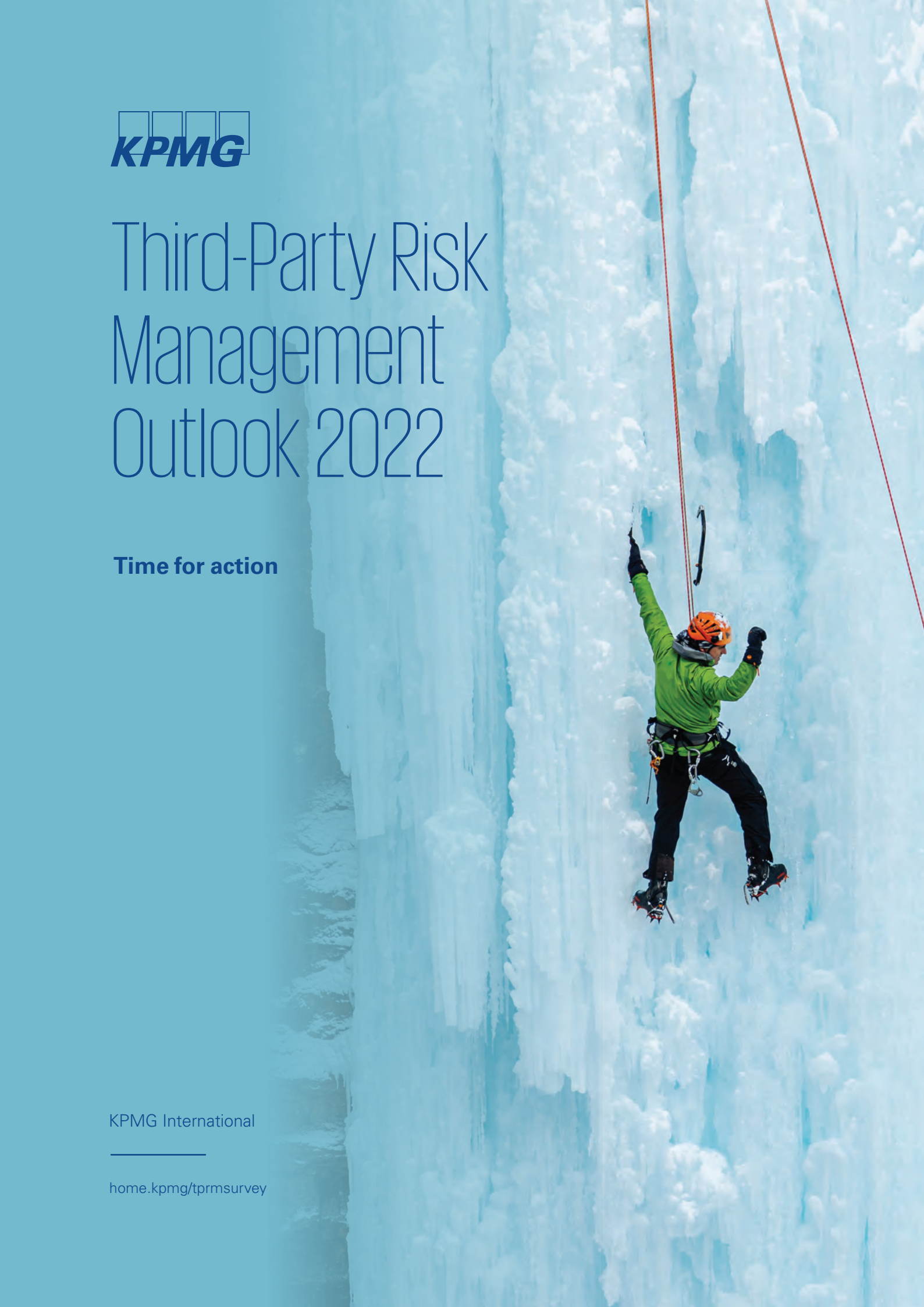
Third-Party Risk Management Outlook 2022

Time for action



KPMG International

home.kpmg/tprmsurvey

Contents

04 Foreword

06 Key themes from the research

12 Priorities and next steps

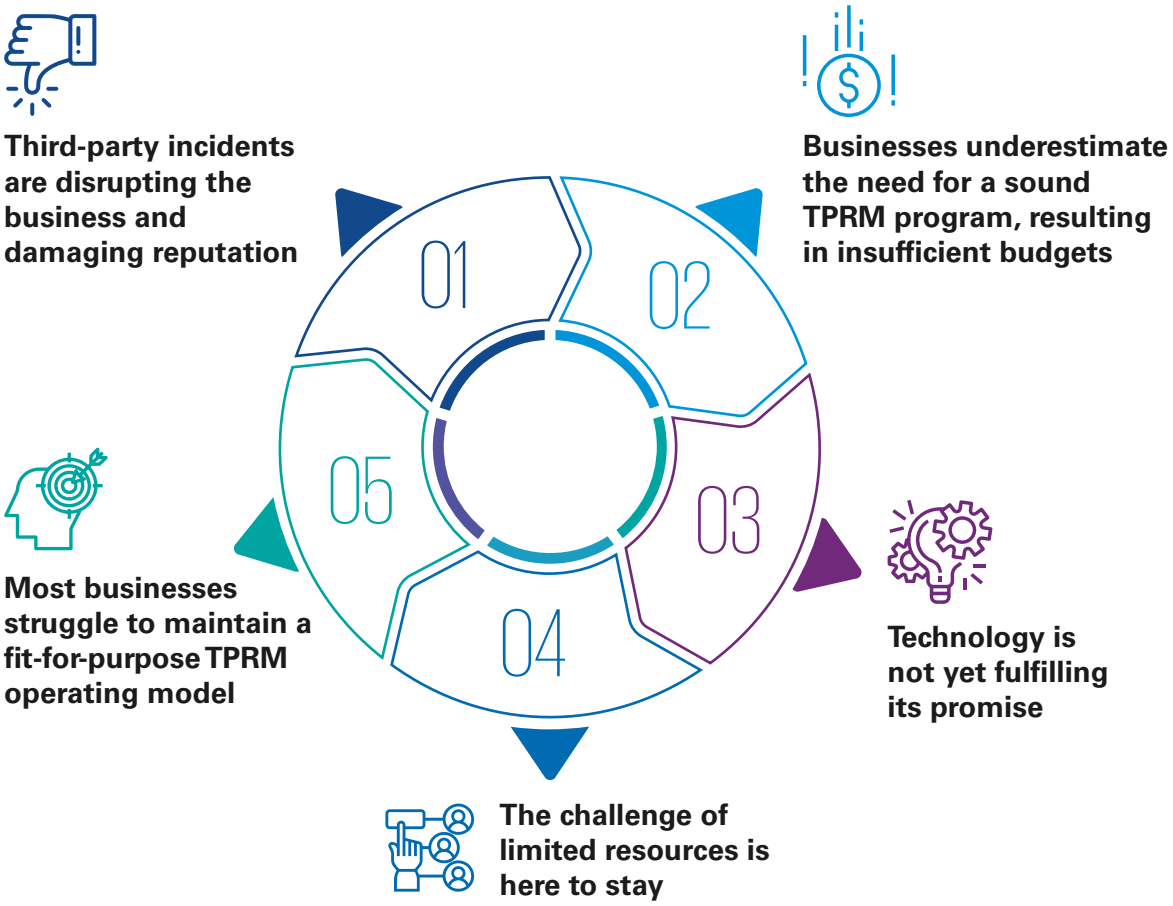
16 About the research

Foreword

As the economic recovery picks up speed, third-party risk management (TPRM) is more important than ever before. Faced with supply chain disruption, cyber threats and growing inflationary pressure, global businesses are assessing their operational resilience and reviewing their dependence on third and fourth parties.

KPMG International's new research — which surveyed 1,263 senior TPRM professionals across six sectors and 16 countries, territories and jurisdictions worldwide — reveals that TPRM is a strategic priority for 85 percent of businesses, up from 77 percent before the outbreak of the pandemic. Nonetheless, the outlook for TPRM presents no shortage of challenges.

Five themes stand out:



01

Third-party incidents are disrupting the business and damaging reputation

Weaknesses in the TPRM operating model, leading to missed opportunities to mitigate risk, are proving to be a major problem for businesses worldwide. Three in four (73 percent) respondents to our survey have experienced at least one significant disruption, caused by a third party, within the last three years.

02

Businesses underestimate the need for a sound TPRM program, resulting in insufficient budgets

Practitioners are held back by limited budgets that see them prioritizing tactical initiatives over strategic improvements. Six in 10 (61 percent) believe TPRM is undervalued considering its enterprise-critical role. If businesses understood the full complexity of a sound TPRM program, rather than narrowing in on its individual components, they could support larger budgets while benefiting from new efficiencies around operational resilience, cyber security and fraud.

03

Technology is not yet fulfilling its promise

Respondents expect to use technology to automate or support 58 percent of TPRM tasks within three years, which will free them to focus on activities that require human review and interaction. Today, however, 59 percent are frustrated by the lack of visibility that their technology gives them around third-party risk.

04

The challenge of limited resources is here to stay

TPRM programs are continuing to evolve while teams contend with a growing body of work. Digital tools will help shoulder the burden, but TPRM's remit is expanding across all risks, domains, and types of third parties. The number of businesses assessing all third parties for environmental risk is, for example, expected to reach 30 percent within three years. A risk-based approach, allocating resources to highest-risk arrangements, would be preferable.

05

Most businesses struggle to maintain a fit-for-purpose TPRM operating model

Respondents largely accept that it was luck, rather than their TPRM programs, which helped them avoid a major third-party incident during the COVID-19 pandemic. In turn, 77 percent believe that overhauling the operating model is overdue.

Our findings demonstrate the need for TPRM leaders to make a step change in their operating models and their approach to third-party risk. This need will likely only grow as supply chains and ecosystems continue to expand and the risk presented by fourth parties creates further complexity.

Strong leadership and the ability to talk the language of the business — reflecting the priorities that business partners themselves set for third parties — is key. Our recommendations, which we set out in Section 3, are designed to support a business environment in which TPRM remains high on the boardroom and management agenda throughout the pandemic recovery. Recognizing the need for action, while cognizant that there is no quick fix to the challenges faced by TPRM executives, we outline depending on your program's maturity a number of focus areas you can explore to drive enhancements to your program.

Key themes from the research

01 Third-party incidents are disrupting the business and damaging reputation

TPRM leaders tell us that, during the pandemic, the board and management began paying even greater attention to the TPRM program and to their overall dependence on third parties.

This board-level scrutiny highlights how disruptions caused by third parties are having a material impact on performance and will likely become more prevalent if steps aren't taken to improve TPRM. To that end, we see a rise in the number of businesses that say that inefficiencies in the program are exposing them to reputational risk — 73 percent say this, up from 68 percent in our 2020 survey.

Third parties are causing disruption and value loss

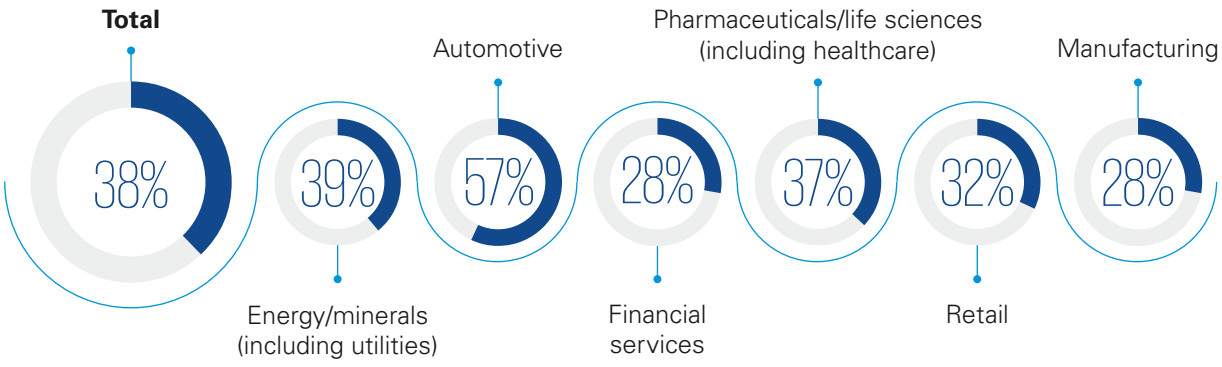
Our research indicates that most businesses have recently experienced business disruption because of a third party. Almost three in four (73 percent) have had at least one major disruption that is directly attributable to third parties, within the last three years alone. Four in 10 (38 percent) have weathered three or more in that time (Figure 1).

Resilience is not the only third-party issue that companies are struggling with. Two-thirds (65 percent) are increasingly concerned that inefficiencies in the billing payment process mean they are not obtaining the full value from service providers. If organizations do not have a mechanism in place to compare service delivery with the terms specified in the contract, for example, they may end up paying in full for a service that was unacceptably delayed or did not meet the required standard. Alternatively, some may have contracts with their third parties that do not specify service level agreements and associated financial incentives.

At the same time, 54 percent believe they have been overbilled by a third party at least once during the last 12 months — an issue that could, potentially, be controlled by implementing a system that flags when the invoiced fee comes in higher than specified in the statement of work.

Figure 1: Businesses are experiencing multiple third-party disruptions

Have you experienced a significant disruption, monetary loss or reputational damage as a result of a third party within the last three years?



Source: Third-Party Risk Management Outlook 2022, KPMG International, January 2022

Fourth parties ramp up the pressure

Alexander Geschonneck, Partner, KPMG in Germany, notes that a growing challenge for TPRM is that businesses are increasingly relying on subcontractors in the supply chain, which presents additional complexity. "Across sectors, fourth parties have been responsible for much recent disruption," he says. "In manufacturing, that might result from shipping failures. More broadly, it could be a security vulnerability at a supplier's cloud provider that results in a cyber incident."

The challenge presented by fourth parties has not gone unnoticed by respondents to our survey. Eight in 10 (79 percent) say that they urgently need to improve how they identify and assess fourth parties in their supply chain and the broader ecosystem, a notable increase from the 72 percent who said this in 2020. The challenge will likely be exacerbated further when there is no contractual arrangement or direct relationship with said fourth parties.

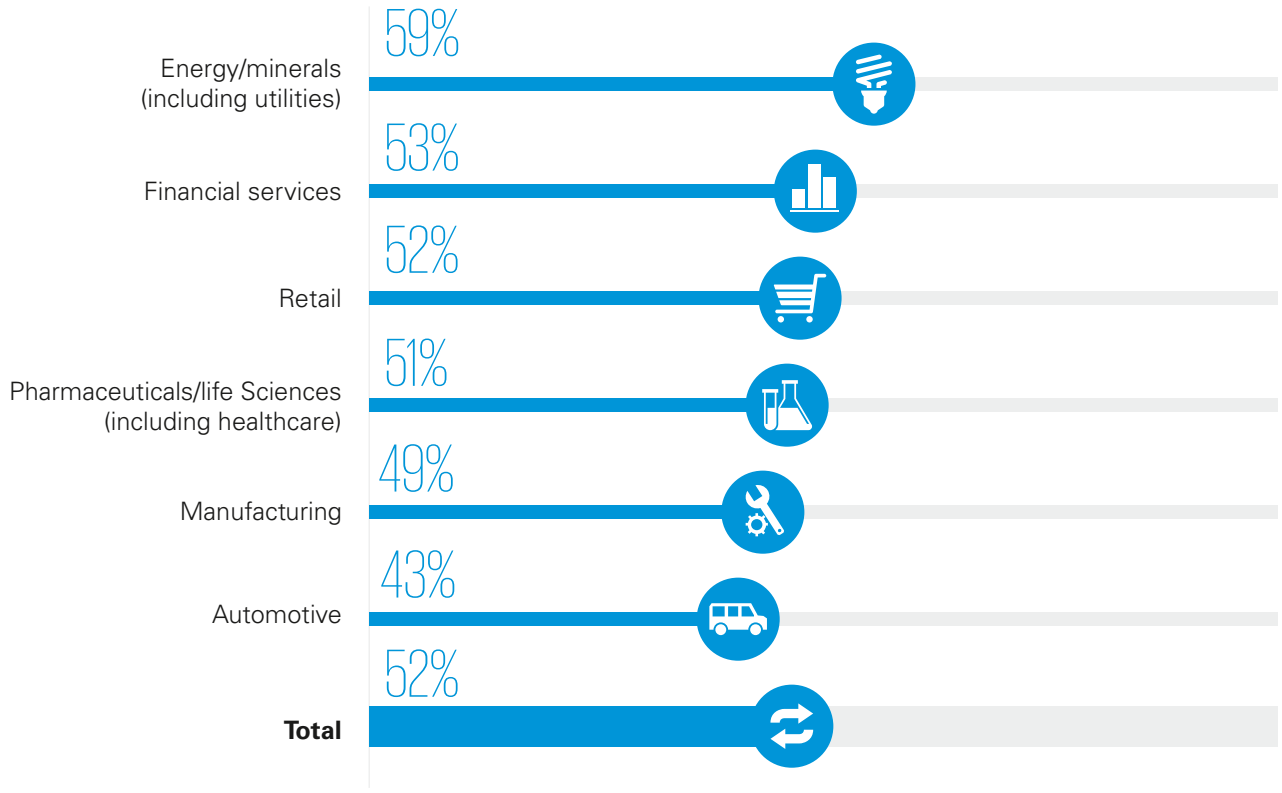
02 Businesses underestimate the need for a sound TPRM program, resulting in insufficient budgets

TPRM executives should urgently review and upgrade their operating models. To do so, they need budget and support from senior leadership. Importantly, this budget needs to be sufficient to meet requirements at an enterprise-wide program level, rather than at the level of individual third-party transactions.

The main stumbling block here is a failure, on the part of the business, to appreciate the full complexity of TPRM. In our survey, 61 percent of respondents believe TPRM is undervalued, given the extent to which the business model relies on third parties. One in two (52 percent) warns that they do not have sufficient capabilities in-house to manage all the third-party risks they face, albeit with some variety across industries (see Figure 2).

Figure 2: Organizations are under-resourced to effectively manage third-party risk

We do not have sufficient capabilities in-house to manage all the third-party risks we face



Source: Third-Party Risk Management Outlook 2022, KPMG International, January 2022

Lack of funding prevents TPRM leaders from uplifting the technology, talent and processes that enable them to create new efficiencies and assess third parties on a strategic, enterprise-wide scale. Seven in 10 (68 percent), for example, say they have a long way to go before they could be described as a strategic partner, supporting major initiatives such as cyber security, environmental, social and governance (ESG), and operational resilience.

Indeed, the limited funding that TPRM does receive is only enough to cover core expenses and tactical investments. In our survey, 63 percent of respondents confirm that their budgets are mainly spent on business-as-usual costs rather than strategic improvements.

Operational resilience needs more TPRM

Operational resilience is one area where TPRM teams could be making a stronger contribution. More than three in four (77 percent) believe they should be playing a much more active role in ensuring business continuity than they are currently. Moreover, just one in five (19 percent) says that operational resilience is a top driver of TPRM activity in their business at the current time.

This, respondents suggest, is a serious oversight considering the potential that can go wrong when inadequate assessment is given to third and fourth parties in the supply chain and how they interact to deliver goods or services to the client.

Greg Matthews, Partner, KPMG in the US views operational resilience as more than just business continuity and believes it should look at multiple factors around the delivery of goods and services, understanding how the value chain can withstand third party, technology, location, people and other disruptions when they often end up occurring together.

Strong, consistent leadership is key. "You need a concerted enterprise-wide approach to define what resilience means, to manage the complexity involved in running services across multiple business units, and to map and understand the people, location, technology, and third parties involved," he explains.

Talking the language of the business

Matthews argues that leadership underestimates the complexity of enabling TPRM across the enterprise. "Leadership teams often expect TPRM to be covered by individual functions such as procurement, specific risk disciplines or business units, and overlook the synergies that could arise from a coordinated approach," he says.

If a more holistic view is factored into the design and build of a TPRM program, showing how other programs depend on TPRM, its scale and scope become clearer, allowing leadership to allocate appropriate budget to deal with the enterprise-wide need.

"The business's top metric is throughput time and taking less time than before to engage a third party," Matthews adds. "But, in order to achieve this, many unglamourous aspects have to be resolved across the organization first, such as roles and responsibilities, data models, technology needs and balancing risk with speed. Solving this requires an enterprise-led view and not a silo-driven approach."

Leadership teams often expect TPRM to be covered by individual functions such as procurement, specific risk disciplines or business units, and overlook the synergies that could arise from a coordinated approach.

03 Technology is not yet fulfilling its promise

TPRM teams are already relying on technology, where possible, to lift the load. Almost half (46 percent) of all TPRM tasks, on average, are supported by technology or process automation to some extent. Executives expect the proportion of supported tasks to rise to 58 percent within three years.

TPRM teams predominantly use workflow solutions to support processes, while across the risk functions connected to TPRM, the use of various platforms and third-party service providers support the execution of due diligence activities.

The expectation-reality gap

Despite TPRM executives' high hopes for technology, feedback suggests that existing tools are often unsatisfactory or burdensome. Many report that they are ultimately unsatisfied by the solutions on offer and that they run into data-related issues. There is also a debate around whether the technology is flawed or whether the underperformance is based on how the technology was implemented. In our survey, respondents flag integration challenges as the second biggest barrier to TPRM transformation, after concerns about data breach.

Above all, lack of visibility remains the primary issue. Six in 10 respondents (59 percent) warn that their technology does not give them "anywhere near the visibility they need" to manage third-party risk across the supply chain. This visibility refers to the different stages of the contracting process, all the way through to understanding which controls are in place within the third party's environment to manage service delivery in line with expectations.

Joy St. John, Director, KPMG in the US notes that visibility is not, however, the only issue. "Executives are also frustrated by the construct of the technology, over-engineering of the program, and by a lack of effective and clear reporting on program performance and third-party performance," she says.

Perfection is out of reach

With the existing limitations in mind, scaling up automation to the extent that respondents are planning can present several new challenges and risks, which could prove counterproductive for stretched TPRM teams.

Fixing the technology aspects of the TPRM program requires an enterprise approach, reflecting that different procurement, contract lifecycle management and vendor performance systems vary and that integrating the underlying data should be dealt with holistically. Teams' expectations around what technology can do for workflow or risk management, for example, need to be managed to make sure that perfection doesn't become the enemy of good.

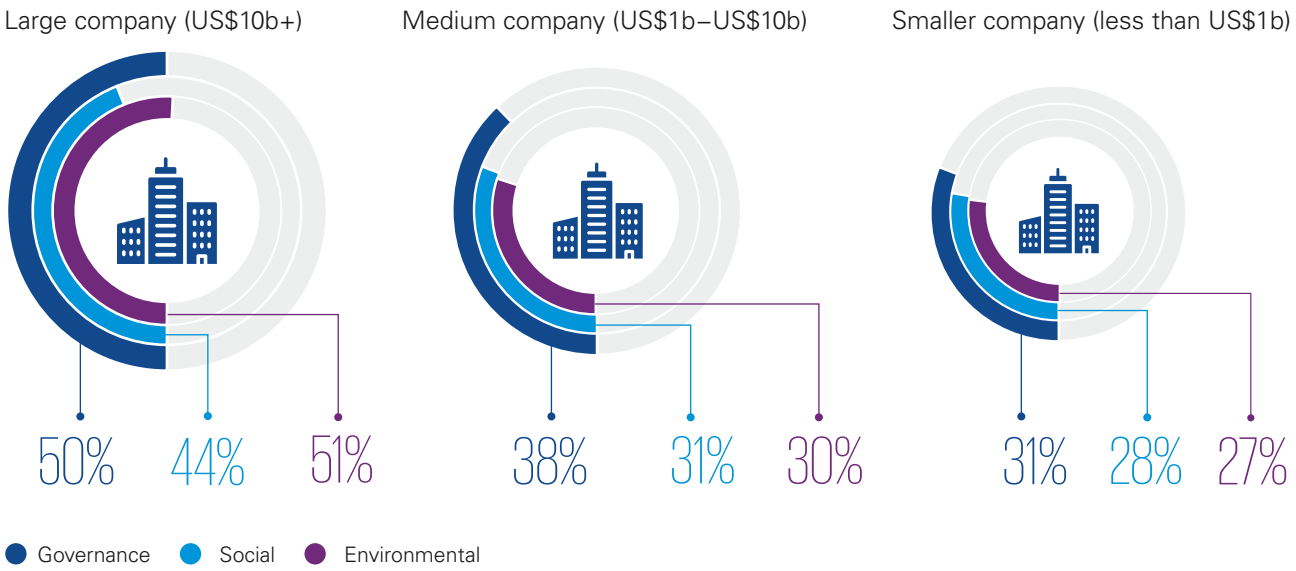
04 The challenge of limited resources is here to stay

Many businesses do not have all the TPRM capabilities they require. Expanding TPRM teams' remit to cover a wider range of risks, and to achieve a deeper understanding of how the risk is managed by each third party, can increase the pressure significantly. One example of the additional pressure comes from corporate ambitions around ESG performance.

In recent years, ESG has grown rapidly in importance, and TPRM's focus on related risks is expected to increase in the years to come. Three in 10 respondents say they are planning to assess all third parties for the environmental risk component of ESG within three years, up from 23 percent who do so today. The proportions are even higher when we break respondents down by size of business, with approximately half of large businesses (i.e., with revenues exceeding US$10 billion) saying they will assess all third parties for each of the three individual ESG risks within the next three years.

Figure 3: Larger businesses are much more likely to assess all third parties for ESG risk

Will assess all third parties for ESG in three years time



Source: Third-Party Risk Management Outlook 2022, KPMG International, January 2022

Pushing back with an alternate approach

"How can organizations achieve this volume when they don't have resources as it is?" asks Gavin Rosettenstein, Partner, KPMG Australia. As technology improves, workflow and automation will likely play a larger role. More immediately, however, adopting a risk-based methodology would allow for a more targeted approach, focused on the different types of arrangements in place and restricted only to the relevant risk types.

"Not all third parties present environmental risk, so assessing all of them can make it impossible to right-size your program and speed up the onboarding throughput time," Rosettenstein explains. "The focus should be on increasing awareness rather than assessing all third parties for environmental risk."

Meanwhile, St. John recommends focusing on the interconnection between ESG and reputational risk. "Companies want to assess third parties to know they're not affiliated with third parties who have a checkered past with regards to ESG, she says. "It may not be necessary to do a full environmental risk assessment. Increasing background checks from a reputational perspective may be all that is required."

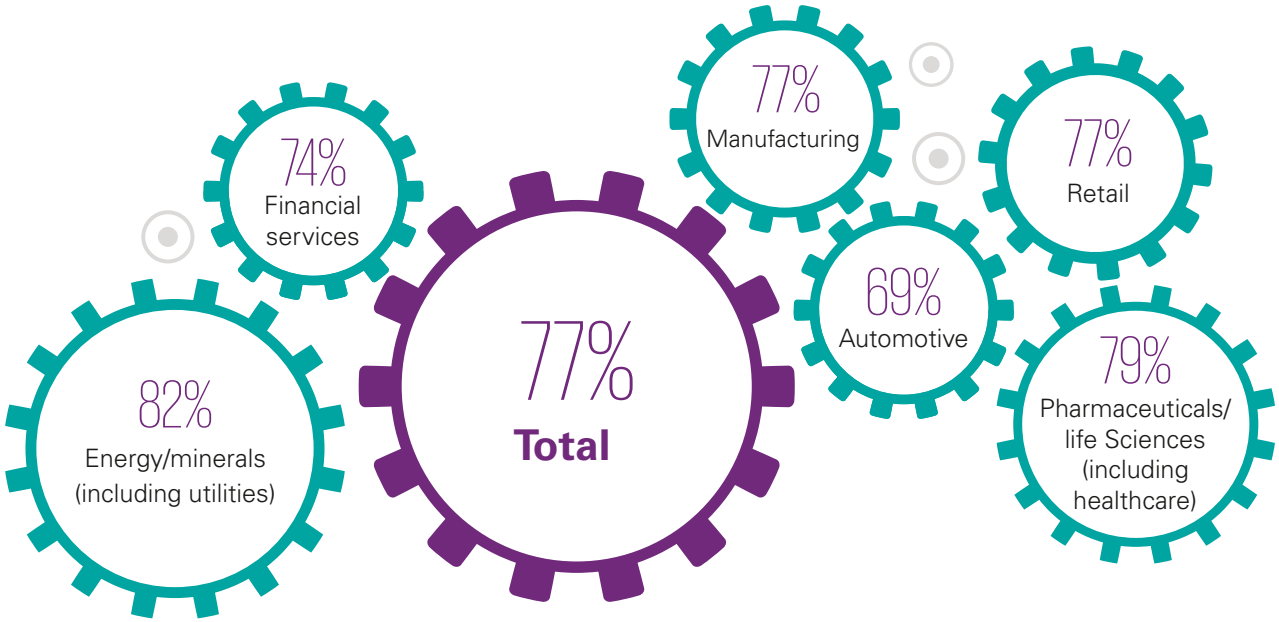
05 Most businesses struggle to maintain a fit-for-purpose TPRM operating model

As our findings demonstrate, companies' TPRM programs are all too often failing to deliver. At the height of the pandemic, as companies reassessed the risk profiles of their third parties and took stock of their exposure, weaknesses in the program became hard to ignore. Today, these weaknesses require urgent attention.

Our findings should be a wake-up call for TPRM leaders. More than one in two (55 percent) respondents believes it was luck, rather than their careful oversight, that enabled them to avoid a major third-party incident during the crisis. More than three in four (77 percent) admit that overhauling the TPRM operating model is now overdue (see Figure 4).

Figure 4: Organizations recognize the need to upgrade their operating model

The pandemic made it clear it's time for us to overhaul our TPRM operating model



Source: Third-Party Risk Management Outlook 2022, KPMG International, January 2022

Time for serious change

"We expected TPRM to become even more of a strategic priority following the pandemic," says Jon Dowie, Partner, KPMG in the UK. "But it's concerning that businesses are not taking TPRM as far as it needs to go. The focus up to now has often been on addressing tactical issues, rather than getting an enterprise-wide fix and engagement across the organization. There's a real need to wake up and sort this out."

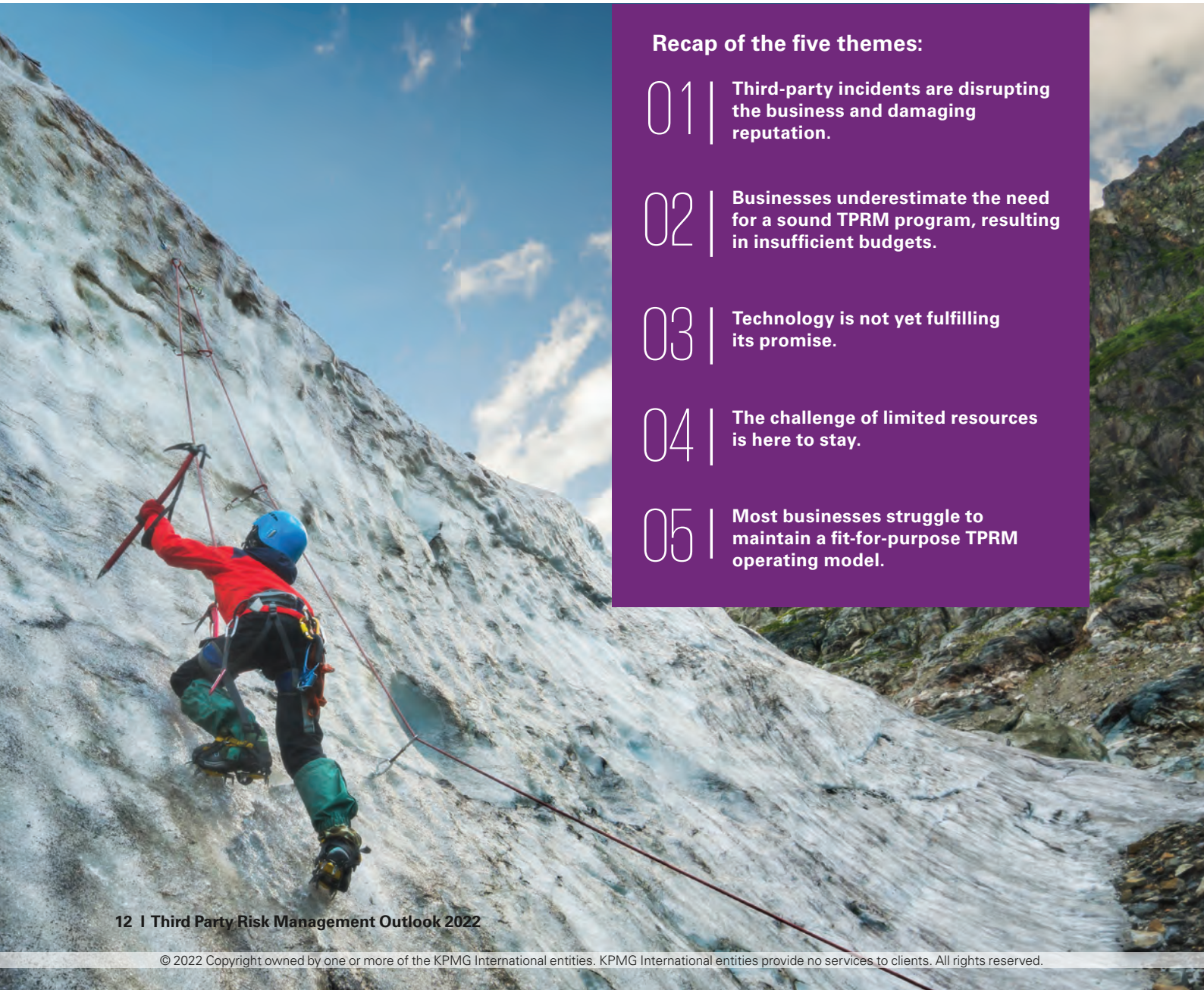
Many organizations have a long way to go before they achieve TPRM maturity and often do not even have the core elements of an effective operating model in place. One of the challenges is that TPRM is a component of a larger program focused on procuring and managing services. Understanding the larger program is key to seeing the overall value of this body of work.

Little more than one in three (36 percent) respondents say their program is well integrated with partner functions such as procurement and legal. Similarly low numbers say they report regularly to senior management or set clear roles and responsibilities across the TPRM program and lifecycle. Such essential elements are vital if TPRM executives are to meet the strategic expectations that the business is putting on them.

In the next section of this report, we consider how to overcome the challenges expressed by our respondents and outline the five critical success factors that are required for a fit-for-purpose TPRM program.

Priorities and next steps

TPRM is expected to remain high on the boardroom and management agenda in 2022 as businesses grapple with new and evolving regulations, complex operating models, fast-growing vendor bases, and other realities of the post-pandemic era such as cyber security and supply chain disruptions.



Recap of the five themes:

01 | **Third-party incidents are disrupting the business and damaging reputation.**

02 | **Businesses underestimate the need for a sound TPRM program, resulting in insufficient budgets.**

03 | **Technology is not yet fulfilling its promise.**

04 | **The challenge of limited resources is here to stay.**

05 | **Most businesses struggle to maintain a fit-for-purpose TPRM operating model.**

There are no quick fixes to the five thematic challenges outlined in this research, especially as budgets are limited and executives find themselves continually prioritizing resources in an evolving business landscape.

What we have observed is that there are generally common focus areas for organizations that are less mature and seeking to put in place a TPRM program as well as for those more mature organizations looking to optimize their program.

Below we highlight a few of these and discuss how you can go about achieving your TPRM transformation.

A. Focus areas for TPRM programs in the early or medium stage of maturity

The imperative for organizations at an early or medium stage of maturity is to establish a program that allows you to manage third parties appropriately. For any organization, below are some of the must-haves when it comes to a viable TPRM program.

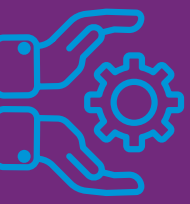
- **Pre-contract to due diligence:** You should complete appropriate due diligence prior to executing the contract. Depending on the industry and service, key risks such as cyber security, business continuity or compliance may be prioritized over other risks.
- **Risk-based approach:** You don't need to look at each third-party engagement with the same level of depth. Considering limited time and resources, you should focus on the third parties that impact the most critical services. As the TPRM program matures, you can expand the scope to cover broader tiers of third-party arrangements as well as additional risk domains.
- **Ongoing monitoring:** For third parties supporting critical services, you should establish an ongoing monitoring plan to assess, over the lifetime of the contract, that the third party is delivering in line with expectations. The control assessment should be done by the relationship owner and overseen by a function responsible for that risk.
- **Program governance:** this focuses on overseeing, monitoring and governing the arrangement, effectively resolving incidents that occur, and managing occasions when a decision is required that is at odds with the stated policy. These types of governance decisions need appropriate policies, along with clear roles and responsibilities, to avoid ineffective challenge and poor decision-making.

B. Focus areas for TPRM programs in the more advanced stages of maturity

Organizations that are at a more advanced stage of TPRM maturity, whose programs are well-established and fully operational, should focus now on optimizing the program. It is often cost pressures and frustrations around the time taken to complete assessments that drive this need.

Optimizing an advanced TPRM program generally focuses on the following areas:

- **Automation:** Organizations are looking to automate the end-to-end workflow, having tools/technologies replace human activity and reducing the time to complete those activities. This can support faster decision-making and assist in managing costs. To complete tasks for various components, you can also leverage industry utilities or feeds to streamline the due diligence process.
- **Risk-based approach:** To further streamline the risk tiering of third-party services, you can tighten the criteria used to delineate something as critical or high risk. This may include:
  - Using specialty programs for homogenous groups of third-party services with a standard risk profile, such as affiliates, to allow for a "light-touch" approach.
  - Proceeding straight to a purchase order when there is nominal risk in a service.
  - Processing the remaining "standard" contracts through the third-party program, but reducing the number of questions associated with each risk category, evaluating the need for on-site/in-person due diligence, and using industry utilities that provide assessment reports covering in-scope areas.
- **Off-boarding and disengagement:** Organizations want to understand how they can exit a relationship in the event of a stressed situation that is not of their doing. They also want to make sure the service continues to be delivered to customers and markets. Mapping specific services to products and processes within the organization is required to help complete the exercise.
- **Service delivery model:** We see an ongoing trend for businesses to establish a unified, enterprise-wide "center of excellence", which may or may not be centralized. The center of excellence is one of the most efficient ways for organizations with limited resources to cover the broad population of third parties. A unified framework supports consistency across the program, enhanced data quality, and accountability between the central team and the relationship owner.
- **Management of fourth parties and affiliates:** In mature programs, fourth parties – as well as intercompany and intracompany transactions – are no longer out of scope. You can benefit from having appropriate controls such as contract documentation and from aligning program steps with those required by the TPRM program.



How KPMG can support TPRM leaders in achieving their goals

TPRM leaders understand that they need a structured and phased approach to achieve the right level of board and management attention and investment. KPMG professionals can support you across the spectrum of needs you may have to achieve your TPRM program goals as laid out below:

Assess

- **Maturity assessment** Rapid current state review of TPRM capabilities; provide observations and recommendations
- **Regulatory review** Gap analysis against relevant regulatory requirements; provide observations and recommendations
- **Business case and roadmap** Prioritize enhancements and size the level of effort required to roll out the program
- **Internal Audit** Three lines of defense (3LoD) co-source

Transform

- **Framework design** Establish or enhance TPRM program and process components; develop program documentation, lifecycle templates and technology business requirements
- **Technology enablement** Configure and implement workflow technology, risk intelligence software and third-party utilities
- **Tuning and optimization** Enhance elements of the TPRM program and process; e.g. metrics and reporting, data analytics or TPRM risk appetite

Run

- **Scenario testing** Third-party business continuity and exit plans
- **Managed services** Operate end-to-end processes for pre- and post-contract screening and monitoring of third parties. Incorporate leading technologies and data sources with leading practice processes delivered by risk domain professionals
- **Third-Party assessments** Execute portfolio of risk and controls assessments pre- and post-contract

1. Assess your requirements and scope

It is always a good start to assess how regulation is evolving across your business's jurisdictional footprint. Depending on your region and industry, we are seeing a number of global regulators looking at third-party risk management from both a broader outsourcing perspective to a more focused view on privacy, cyber security, ESG, etc.

Ensuring compliance with regulations such as these and being prepared to respond to regulator queries at any time to avoid financial or reputational damages is often a key requirement of the program.

An effective TPRM program relies on the integration and steady operation of several components, spanning people, process, delivery model, governance, data, and technology. Recognizing how your program stacks up across these areas will give you a picture of your organization's current level of maturity. In doing so, you can identify strengths and weaknesses on the component level while making a judgment as to whether the overarching operating model is fit for purpose, sustainable and well-integrated.

As you define your aspirations and maturity target, it is worth noting that you do not need to achieve comparable maturity across all components of TPRM. Depending on prioritization, some components may be more developed than others to meet the needs of the business.

2. Transform your program

KPMG has invested significant time and resources globally in designing and developing a model end-to-end TPRM program based on our collective cross-industry and global experience.

Our KPMG Powered Enterprise Risk - Third-Party Risk Management program represents an 80 percent solution of "what good looks like", allowing for configuration by clients. It is enabled and supported by various assets, including governance structures, policies, role and responsibility matrices, scoring methodologies, questionnaires, and reporting templates.

Although the model is technology agnostic, we have built it using leading governance, risk, and compliance (GRC) platforms to support rapid implementation and enhance the program it is supporting. As there is no one-size-fits-all approach to TPRM, we believe that calibrating and adjusting a full suite of components for a mature organization is vital to the program's success.

Uplifting an enterprise-wide TPRM program is a major initiative that requires sufficient resources, and the full commitment of senior executives, to become a success. You need to be clear about where you're going, how you're going to get there, and what you need to complete the journey.

With that in mind, it is worth assuming at the outset that you have underestimated the amount of effort and operational interdependencies that will be required, and to try to secure additional investment upfront. Technology automation and capitalizing on the digitization trend is something we expect to continue in the coming years.

In response, KPMG has developed relationships with key technology and industry utility providers to help drive efficiencies around process and due diligence automation, and the continuous monitoring of controls. We are driving greater integration across TPRM, procurement, contract lifecycle management and other risk functions to take advantage of advances in these areas and help improve the user experience.

3. Run your program but plan resources for the unexpected

In our experience, a fully operational TPRM program requires more resources to execute the pre- and post-contract assessment and monitoring activities. TPRM capabilities encompass a cross-organizational operating model and practitioners need a wide set of skills to manage the full suite of risks. This can make it harder to secure all capabilities internally.

As our survey highlights, organizations are challenged by resource availability and skill and are seeking better and smarter ways to manage TPRM activities. Some use a multitude of technology enablers and alternate delivery models to address these capability gaps and benefit from efficiencies.

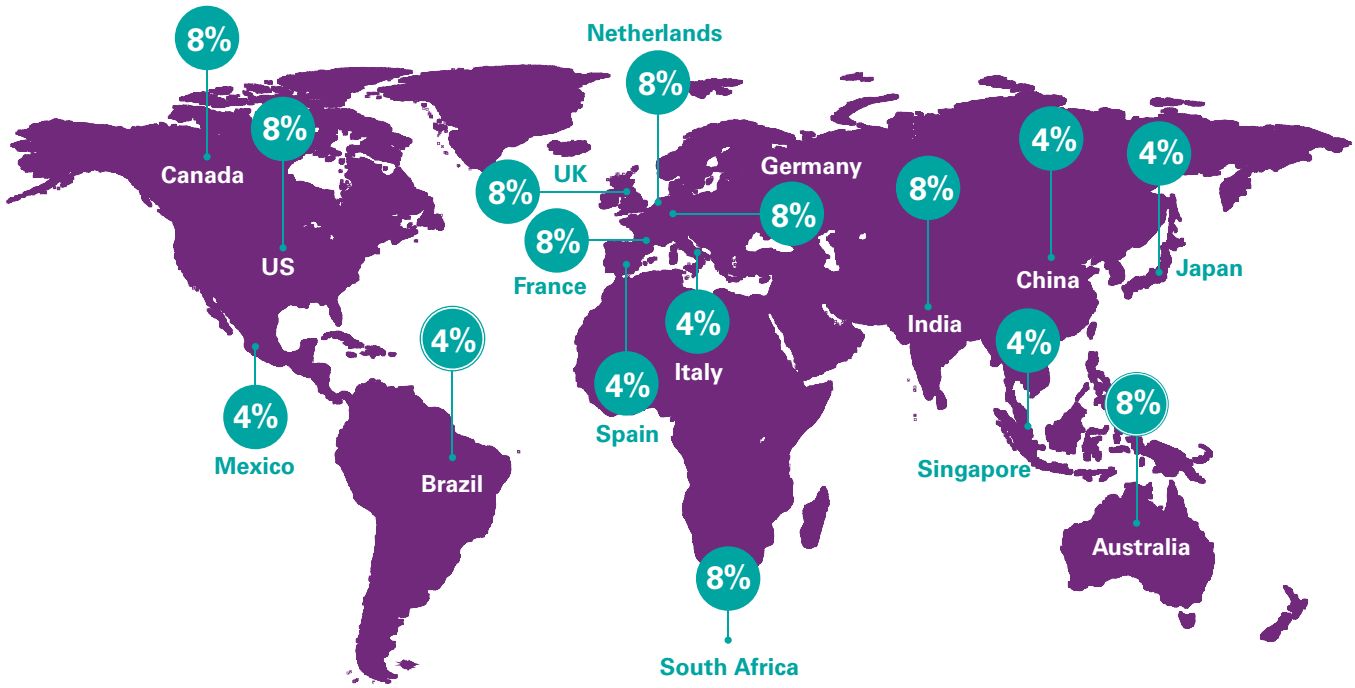
Given our strengths in risk and compliance along with our global footprint, clients frequently ask us to execute the ongoing risk assessment components of their TPRM program, including cyber reviews, control assessments, sanctions and anti-bribery, and corruption reviews, among others. This allows for momentum to be established around the program while helping to manage costs.

KPMG's global TPRM team stands ready to support you build your TPRM program safe in the knowledge that good risk management practices are ultimately good for your business, customers and communities. Please contact us to see how we can help you.

About the research

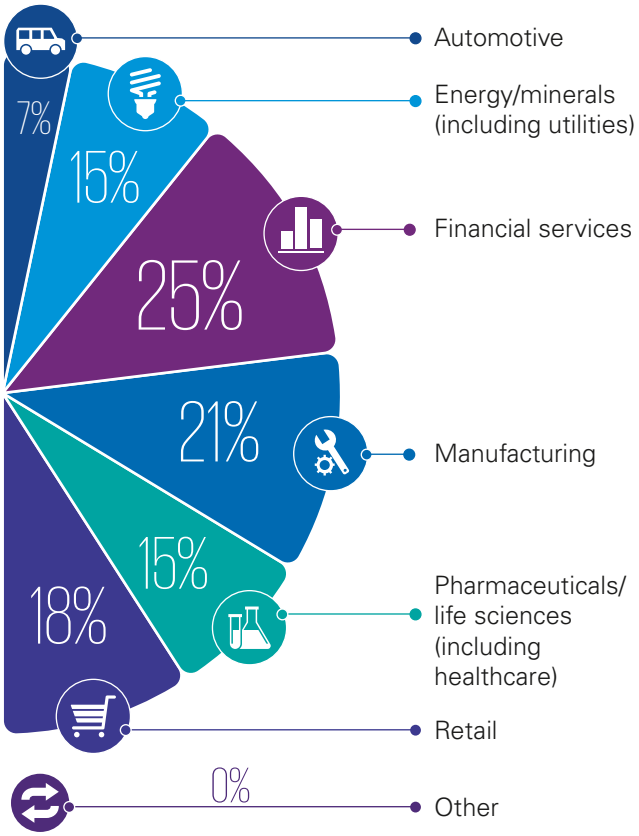
KPMG conducted an online survey of 1,263 senior TPRM executives, all of whom worked for major businesses across 16 countries, territories and jurisdictions and six industries worldwide.

In which country, territory or jurisdiction does your company primarily operate?

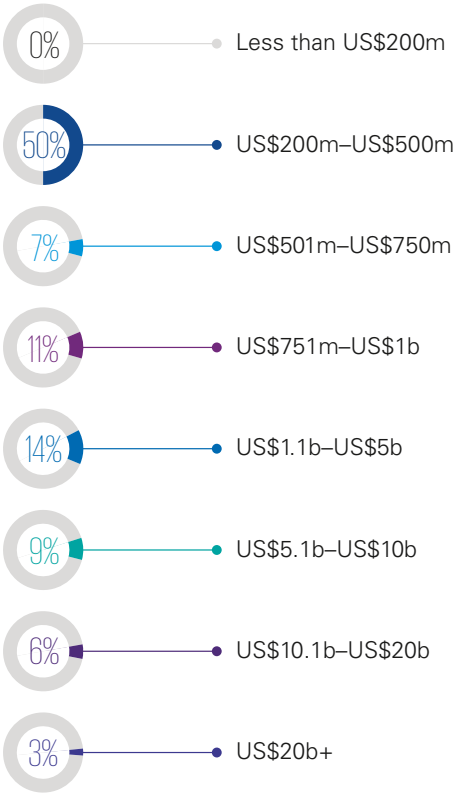


Source: Third-Party Risk Management Outlook 2022, KPMG International, January 2022

In which sector does your company operate?



What is your organization's total global annual revenue?



Source: Third-Party Risk Management Outlook 2022, KPMG International, January 2022

Your Swiss contacts

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich
Switzerland

kpmg.ch

Pascal Sprenger
Partner, Financial Services,
Regulatory & Compliance,
Member of the Board of Directors
psprenger@kpmg.com
+41 58 249 42 23

Reto Gareus
Partner, Financial Services,
Regulatory & Compliance
rgareus@kpmg.com
+41 58 249 42 51

Philippe Fleury
Partner, Office Head Geneva
pfleury@kpmg.com
+41 58 249 37 53

Anne van Heerden
Partner, Head of Forensic
annevanheerden@kpmg.com
+41 58 249 28 61

Sergio Galanti
GRC Technology Advisory
sgalanti@kpmg.com
+41 58 249 69 12

Contributors

Joy St. John
Director, KPMG in the US

Zeynep Turesin Soylu
Associate Director, KPMG Australia

Nicole Trawick
Manager, KPMG in the US

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