KPMG

Achieving resilience in third-party risk management

2026 global third-party risk management survey

kpmg.com

We are delighted to present the results of KPMG's latest global third-party risk management (TPRM) survey.

As organizations increasingly rely on third parties — such as vendors, suppliers, service providers, and technology partners — to support critical operations, managing third-party risk has become a strategic priority.

Rapid digital transformation, expanding global supply chains, heightened regulatory expectations, and growing cybersecurity threats have significantly reshaped the TPRM landscape.

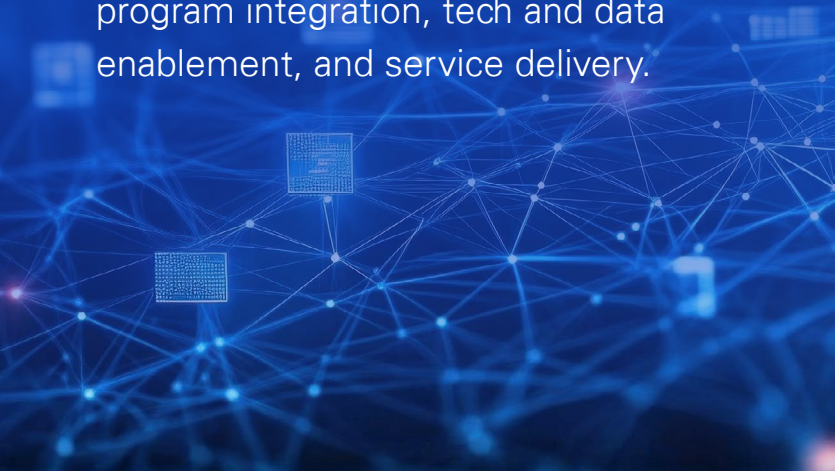
Organizations are now expected not only to identify and assess risks but also to continuously monitor, respond, and adapt to emerging challenges across the third-party lifecycle. And yet, most clients tell us they don't get this right all the time as resources are often bogged down over assessing low-risk third parties rather than focusing on third parties that present real risk.

Against this backdrop, our survey explores the latest trends, practices, and challenges in third-party risk management. It provides insights into how organizations are evolving their TPRM frameworks, adopting new technologies, using external providers, integrating risk functions, and responding to regulatory and operational pressures. It also offers strategic recommendations for managing third-party risk with an eye toward strengthening resilience and creating value.

Alexander Geschonneck
Global Lead, Forensic
KPMG International

Roy Waligora
Global Lead, Third Party Risk Management
KPMG International

Effective, efficient third-party risk management (TPRM) is increasingly crucial — and challenging — in today's complex business landscape. KPMG's global TPRM survey provides a blueprint for building a resilient and future-ready TPRM program to support moving beyond today's reactive approaches. Read the results of the survey to discover future-ready approaches for governance and program integration, tech and data enablement, and service delivery.



Executive summary

Third-party risk management (TPRM) is at a tipping point. For years, leaders have acknowledged the growing importance of their third-party ecosystems, and an opportunity is emerging to bridge the gap between awareness and action with modern capabilities.

The global TPRM survey, which gathered insights from 851 professionals across industries and geographies, reveals a clear opportunity: While leaders acknowledge the high stakes, there is room to enhance execution. The potential benefits of proactive measures are significant, as a third of organizations suffered monetary loss or reputational damage in the past three years alone and 28 percent faced supply chain disruptions.

In a world defined by constant disruption, moving beyond checklists to build true, proactive resilience is the way forward.

The data reveals opportunities to improve and build on current efforts. Here is a sample of key findings:

Regulatory compliance/Cyber risk

Regulatory compliance and cyber risk — both critical and immediate threats — dominate attention, suggesting programs have an opportunity to develop capabilities to look around the corner and manage the next wave of risks before they hit.

Integration

With only 53 percent of TPRM programs "mostly integrated" with enterprise risk management (ERM) — and just 18 percent "fully integrated"— there is a significant opportunity to create an enterprise-wide view of risk.

Scalability

Truly scalable, strategic TPRM operating models are an emerging trend: Many organizations are outsourcing discrete, high-volume tasks, creating a path toward end-to-end managed services, which are in place in just 5 percent of organizations.

Leveraging AI

More than half of organizations are exploring artificial intelligence (AI), and with 22 percent finding it "very effective," there is a clear opportunity to better translate technology investments into tangible value.

Data quality

As only 15 percent of leaders express high confidence in the data that underpins their program, improving data quality presents a foundational opportunity to enhance TPRM effectiveness from the ground up.

These findings are a clear signal of the value of moving forward boldly with efforts to modernize and enhance TPRM programs. Resilience isn't a goal you achieve, it's a muscle you build. It requires weaving risk management into the core of your strategy, operations, and culture through integrated systems, smart technology, and shared ownership across the business.

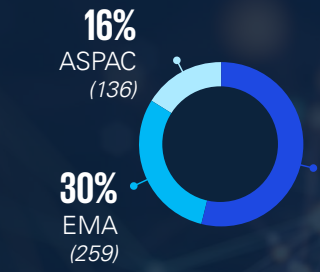
This report aims to cut through the noise, distilling survey insights into five key themes and providing practical guidance that risk, compliance, and technology leaders need to build a future-ready TPRM program.

Methodology

In 2025, KPMG conducted a web-based survey of 851 participants from diverse regions (the Americas, Europe, and Asia-Pacific), company sizes, and sectors such as healthcare, technology, financial services, manufacturing, retail, and energy. The respondents included directors, vice presidents, heads of departments, C-level executives, and managers directly or indirectly involved in TPRM. The survey explored TPRM program maturity, system/tool usage, risk assessment, lifecycle management, resilience, data quality, and technology adoption. We analyzed the results by revenue, sector, function, regulation level, and geography.

Respondent overview

Organization's region



Sector

- 21% Healthcare and life sciences *(178)*
- 19% Technology, media and telecommunications *(164)*
- 19% Financial services *(165)*
- 16% Industrial manufacturing *(139)*
- 12% Consumer and retail *(103)*
- 11% Energy, natural resources and chemicals *(96)*

Current position

- 32% Director/senior director *(273)*
- 26% Vice president/senior vice president *(218)*
- 22% Head of department *(187)*
- 17% C-level *(144)*
- 3% Manager/senior manager *(29)*

Annual spend on third parties

(81)	<US$10 mn	10%
(122)	US$10–49.9 mn	14%
(151)	US$50–99.9 mn	18%
(255)	US$100–499.9 mn	30%
(242)	>US$500 mn	28%

Annual revenue

(232)	<US$5 bn	27%
(179)	US$5.1–10 bn	21%
(194)	US$10.1–20 bn	23%
(242)	>US$20 bn	29%

Function

- 39% Enterprise risk management *(331)*
- 20% Information security risk *(171)*
- 20% Compliance and legal *(173)*
- 14% Operations and logistics *(55)*
- 6% Finance and audit *(121)*

Level of involvement in TPRM

- 56% Directly involved in managing or overseeing TPRM activities *(474)*
- 44% Provide input or support but am not directly responsible *(377)*

Key themes that emerge from the survey findings

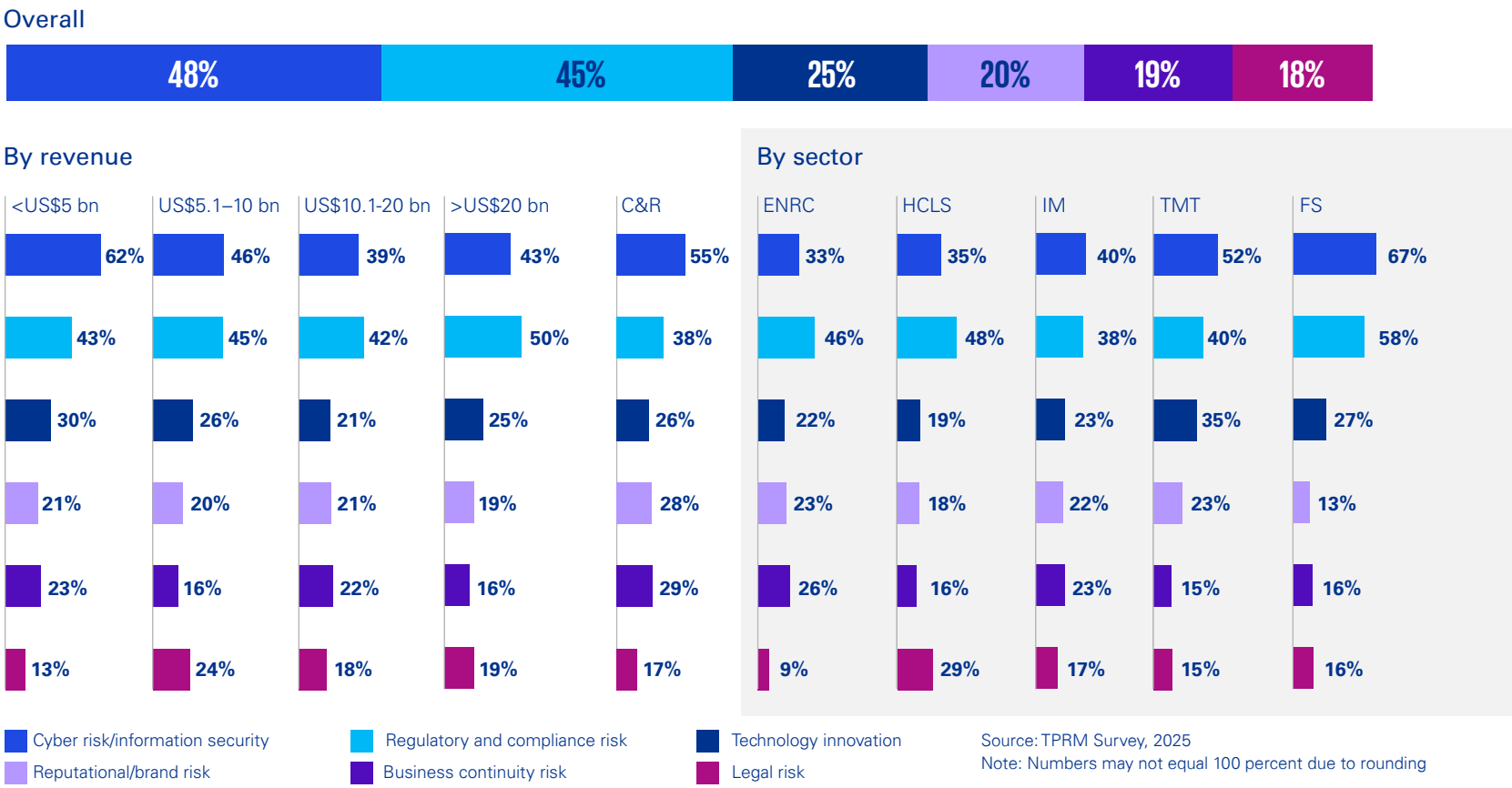
Compliance and cybersecurity: Twin pillars of TPRM strategy

Regulatory compliance and cyber risk continue to dominate TPRM strategy, with 48 percent of survey respondents citing cyber risk as the top driver and 45 percent pointing to compliance. For most organizations, TPRM strategy is still driven by defense. This makes sense: a single vulnerability in a third party can quickly ripple across the entire business, grinding operations to a halt. These priorities reflect a growing awareness that third-party vulnerabilities can rapidly escalate into enterprise-wide threats. This sense of immediacy is reinforced by regulatory expectations and framework-driven mandates across the globe that require companies to scrutinize their third-party relationships.

Spending priorities mirror these concerns — although investments often fall short of delivering holistic risk management. Risk assessment and due diligence (52 percent) and technology/tools for TPRM (51 percent) top the list for TPRM spend categories, followed closely by cybersecurity/data protection (49 percent) and regulatory audits (45 percent).

Exhibit 1. Cyber and regulatory risks dominate TPRM strategy

What risks have grown in importance within TPRM in the last few years?



Source: TPRM Survey, 2025
Note: Numbers may not equal 100 percent due to rounding

Cyber risk has heightened importance to smaller organizations, according to the survey. With more limited resources, smaller companies may find that the cyber function is often their main defense against cyber threats. In contrast, larger well-funded organizations have the resources to expand enterprise-wide capabilities to manage risks in a more holistic way and reduce overall exposure.

Sector-specific nuances also impact drivers of TPRM strategy as well as spending priorities. For example, financial services firms are driven by stringent regulatory mandates, while life sciences organizations face complex compliance demands tied to diverse third-party relationships. Meanwhile, manufacturers are increasingly incorporating several elements into their TPRM frameworks, such as environmental, social, and governance (ESG) factors; human rights; and sustainability. In many sectors, understanding the origin of parts and materials is critical for navigating tariffs and trade compliance as well as complying with regulatory efforts to uphold sourcing standards.

The wide range of third-party risks facing companies, and the numerous and varied priorities of their TPRM programs, reflect challenges of scale and complexity. Regardless of industry, the sheer number of third-party risks is increasing significantly as third party ecosystems grow more interconnected — making the need for tailored approaches based on risk level more urgent. Modern businesses rely heavily on third-party partnerships to create value and drive innovation, but they are expanding faster than organizations can manage the risks.

According to KPMG research, 83 percent of executives plan to expand their partner networks in the next one to three years, yet 71 percent admit that they have trouble getting their partners to align on goals.[1]

Based on the extensive experience of KPMG professionals in helping clients design and manage TPRM programs, many organizations with tens of thousands of vendors attempt to screen them all, even though only a smaller portion — often 10 to 20 percent — represent higher-risk relationships that merit deeper scrutiny. This creates a significant opportunity to redirect effort toward the areas that matter most.

Another critical focus area is developing "Nth-party" awareness — looking beyond immediate third parties to the vendors they rely on. "Nth-party" visibility is the only way to spot and manage concentration risk, such as over-reliance on third parties in a specific geography. Many companies lack this visibility, but need it to make informed risk appetite decisions, such as whether to continue with a vendor, develop a contingency plan, or exit the relationship.

Strategic recommendations for managing the expanding third-party risk universe with resilience:

Adopt risk-based due diligence: Focus on service type and third-party exposure, not just geography, to concentrate efforts on the highest-risk relationships.

Integrate ESG: Incorporate ESG and human rights considerations into onboarding and monitoring to align with evolving regulatory and stakeholder expectations.

Leverage AI and automation to elevate your talent: Streamline intake, reduce duplication, and accelerate assessments to improve efficiency and focus resources on strategic risk management.

Improve data governance: Enhance data quality and system integration to support reliable, data-driven decision-making and manage concentration risk.

Align with global standards: Meet global regulatory expectations while avoiding overly complex processes that dilute efficiency and effectiveness.

[1] "Accelerate growth and innovation with the right partner ecosystem," KPMG LLP, 2025.

Regulatory requirements and scrutiny are rising

United States

- Telecom — FCC Supply Chain Security
- EO 14028 Software Supply Chain Security
- Financial Services — Interagency Guidance On Managing Third Party Risk
- Life sciences — Food and Drug Administration
- Privacy — Central Consumer Protection Authority
- Healthcare — Health Information Technology for Economic and Clinical Health Act
- Power — North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- Across sectors — the DOJ updated guidance on Corporate Compliance Programs

Canada

- Privacy — Personal Information Protection and Electronic Documents Act
- Financial Services — OSFI Guideline B–10

Europe

- Telecommunication — Toolbox For 5G Security
- Financial Services — DORA, EBA Outsourcing Guidelines
- CII — NIS2
- Healthcare — European Medicines Agency requirements on TPRM
- Privacy — General Data Protection Regulation

India

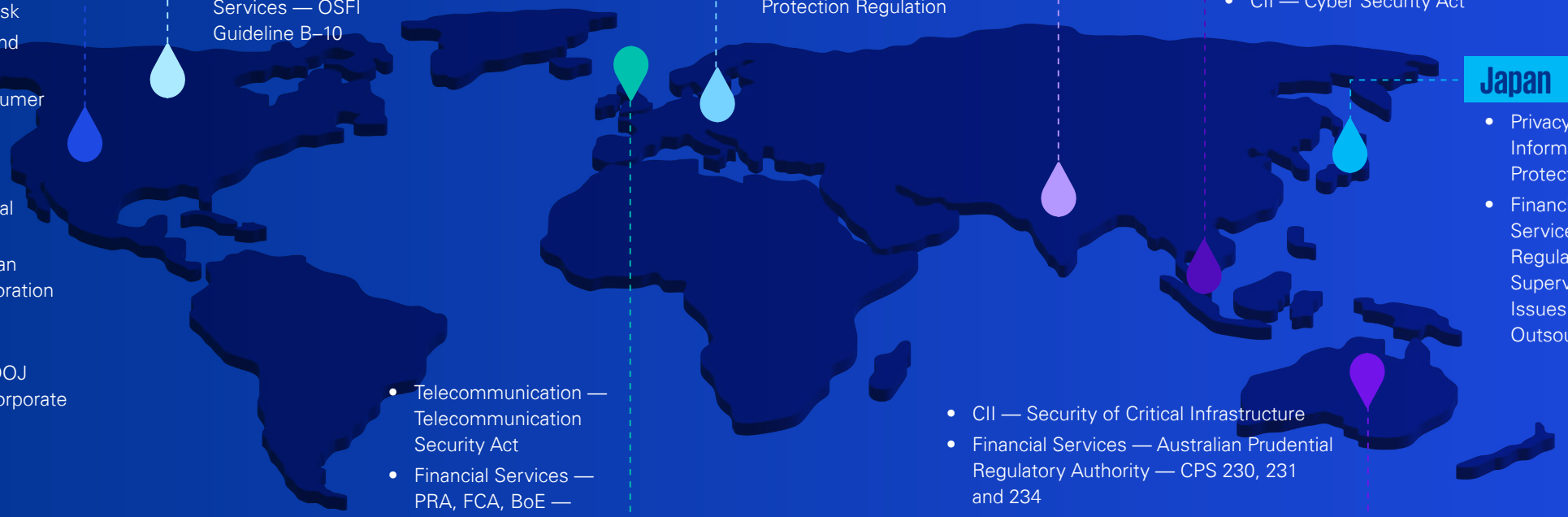
- Financial Services — RBI Guidance On Management Third Party Risk

Singapore

- Financial Services — MAS Outsourcing Notice
- CII — Cyber Security Act

Japan

- Privacy — Personal Information Protection Act
- Financial Services — Regulatory And Supervisory Issues Relating to Outsourcing



United Kingdom

- Telecommunication — Telecommunication Security Act
- Financial Services — PRA, FCA, BoE — Operational Resilience SS1/21 / SS2/21

Australia

- CII — Security of Critical Infrastructure
- Financial Services — Australian Prudential Regulatory Authority — CPS 230, 231 and 234
- Telecommunication — Telecommunications Sector Security Reforms

Integration challenges: TPRM and ERM still speak different languages

Enterprise risk management (ERM) focuses on high-level strategic threats, while TPRM is often managing day-to-day vendor data. This creates a disconnect. Despite widespread recognition of the need for holistic risk management, integration between TPRM and ERM remains fragmented. Seventy-eight percent of organizations report their programs as "mostly integrated" and 71 percent have achieved full integration. Yet organizations face a persistent challenge: aligning TPRM with risk functions in a way that is both strategic and operationally coherent.

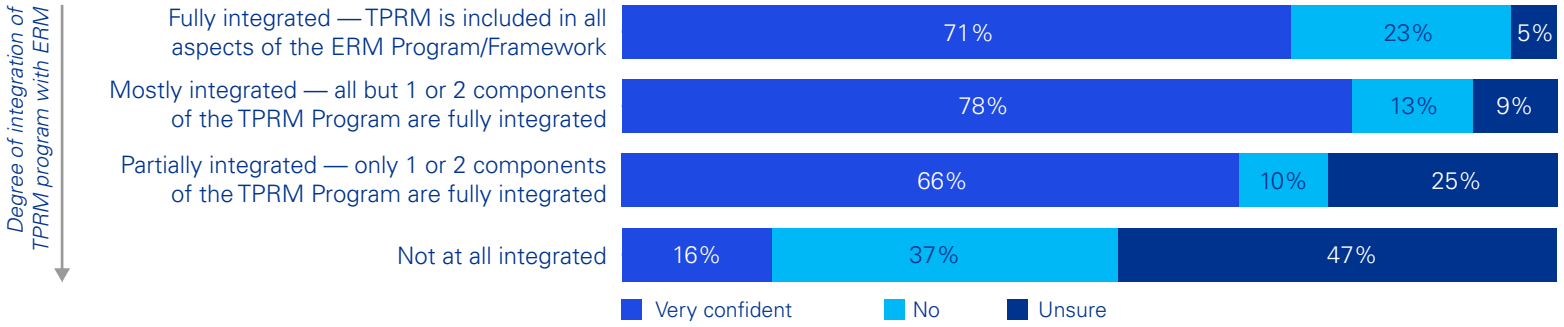
In practice, "mostly integrated" often means that TPRM data feeds into high-level ERM dashboards or reporting frameworks, but lacks deep linkage across systems, processes, and decision-making. ERM is focused on "top of the house" risks that could impede strategy, whereas TPRM is often more transactional, dealing with a high volume of third-party data. Further, TPRM ownership is distributed across many organizations — either "by committee" or with portions of programs led by separate teams, such as procurement, supply chain, cyber, and TPRM, rather than being housed under a broader risk umbrella. This structural separation leads to different languages, priorities, and a lack of a unified risk perspective.

"For a mature organization, integration is all about focus and prioritization — getting the right resources, hiring the right people, deploying the right technologies, and developing a strategy and executing against it."

— Srijit Menon
Partner, KPMG India
Global Lead, Third Party Security

Exhibit 2. There is room to improve integration of TPRM and ERM programs

Level of TPRM/ERM program integration and future integration plans



Source: TPRM Survey, 2025
Note: Numbers may not equal 100 percent due to rounding

The divide is also philosophical. TPRM is often viewed through two lenses: the compliance side, which focuses on risk of harm (e.g., financial crimes, cyber threats, bribery, compliance), and the procurement/supply chain/finance side, which seeks to execute transactions faster, better, and cheaper. Without a shared understanding of risk across these domains, integration falters.

To bridge this gap, leading organizations are embedding TPRM into their business processes (e.g., source-to-pay) and aligning it with enterprise strategy and risk program design. This shift requires more than policy alignment — it demands technological integration, shared taxonomies, and cross-functional governance. The KPMG TPRM framework, for example, helps organizations assess their current maturity and chart a path toward optimal integration, supported by automation and delivery models that bring stakeholders together across cyber, compliance, finance, and operations.

Technology also plays a pivotal role. While 71 percent of organizations plan further integration over the next three years, only 17 percent rate their TPRM data as fully reliable. This data quality gap undermines efforts to consolidate reporting and conduct integrated risk assessments or rely on the work of others.

Strategic recommendations for integrating TPRM and ERM:

Clarify integration goals: Define what full integration looks like — beyond dashboards — to include shared controls, unified assessments, and joint decision-making.

Break down silos: Establish cross-functional governance structures that align TPRM with ERM, compliance, cyber, procurement, supply chain, operations, and information technology.

Invest in data quality: Prioritize data completeness and accuracy to support reliable risk reporting and analytics.

Leverage technology thoughtfully: Use automation and AI to streamline workflows but ensure tools are embedded in broader risk frameworks.

Align TPRM with business processes: Integrate TPRM into procurement and finance processes to ensure risk is managed strategically, not just reactively.

> "When it comes to third-party risk, companies are chasing effectiveness, efficiency, and experience all at once. The challenge is making sure you're not just ticking boxes for compliance, but building a process that's resilient, scalable, and delivers real value for both your business and your vendors and partners."

— Joey Gyengo
Principal, US Third Party Risk Management Lead, KPMG US

Managed services and outsourcing: Scaling TPRM with external support

More than 80 percent of organizations report using managed services, outsourcing, or both to execute core TPRM activities — from due diligence and onboarding to monitoring and remediation. This extends beyond professional services to risk technology and intelligence tools. However, the adoption is not all-encompassing; only about 5 percent have adopted end-to-end managed services. Rather, most organizations opt for partial models, leveraging external support for the high-volume assessment portion of the lifecycle rather than end-to-end services. For instance, 44 percent of respondents use managed services for ongoing monitoring and 27 percent outsource due diligence. This allows them to better manage a large volume of third parties and improve risk management effectiveness and efficiency.

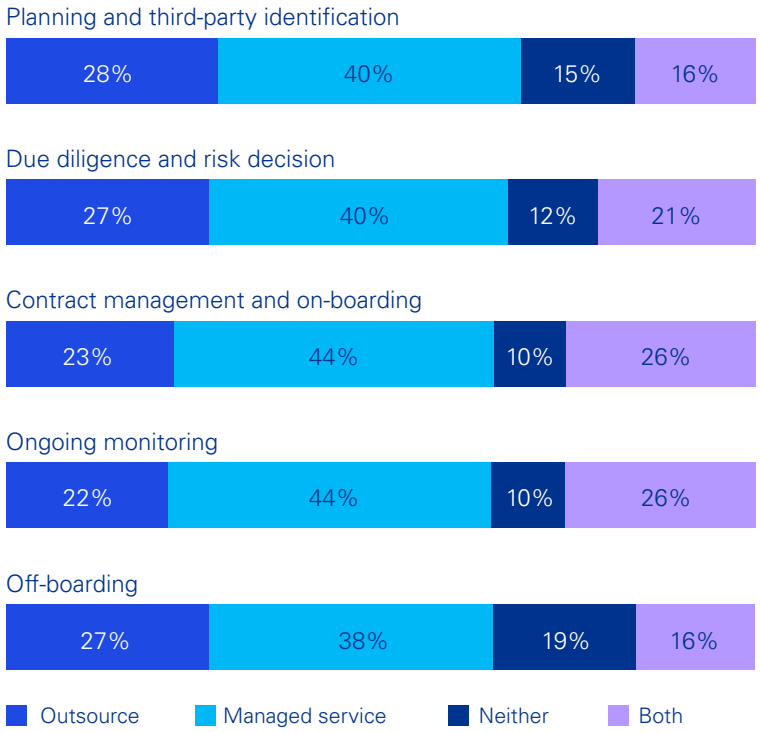
Concerns about losing control and sharing proprietary data are significant barriers to wider adoption of outsourcing, cosourcing, and managed services. Some organizations view their third-party ecosystem as a competitive advantage and are hesitant to share that information. As the thinking around risk management-as-a-service evolves, there's a growing willingness to outsource, but organizations remain cautious about functions they consider core to their business.

While end-to-end managed services remain rare, interest is growing — particularly among organizations seeking to manage process complexity and reduce costs through outsourcing or cosourcing. This is not only a reflection of the complexity of TPRM and the resource constraints faced by internal teams, but a signal of several broader market trends.

For one, the maturation of AI is propelling more companies to shift to partner-based service delivery models for third-party risk management. While organizations are increasingly embedding AI to accelerate individual TPRM tasks, many do so without a holistic optimization strategy, leading to a fragmented "patchwork" of tools that can hinder end-to-end efficiency. By engaging a managed services provider, organizations can replace a fragmented, internally managed collection of tools with a single, pre-integrated platform that is optimized for the entire TPRM lifecycle.

Exhibit 3. TPRM programs largely rely on managed services, particularly for contract management & onboarding

What specific aspects of your TPRM program do you outsource or use managed services for?



Notes: (a) "Other" category is not included in the graphical representation due to low number of responses, (b) Totals may not equal 100 percent due to rounding
Sources: TPRM Survey, 2025

Also driven by advances in AI, the TPRM delivery model is shifting from an hours-to-deliver-based approach to one focused on outcomes. Managed services providers are at the forefront of this evolution, offering tech-enabled, scalable models designed to deliver measurable results like efficiency gains and risk reduction, rather than just billable hours.

Ultimately, while use of full-scale managed services is not yet the norm, it looks poised to grow as organizations mature their TPRM processes and seek scalable, cost-effective solutions, and trustworthy partners.

As organizations adopt outsourcing, cosourcing, and managed services, effective oversight is non-negotiable. To succeed, organizations must have competent people in place to manage the provider relationship, design a program that meets their specific needs, and continuously review and challenge the outputs. Strong project management and governance are essential to maintaining control and ensuring the managed service delivers on its promises.

Of course, readiness to shift toward new service delivery models is often dependent on sector. For example, financial services firms, with their large-scale know-your-customer programs and mature risk functions, are more accustomed to outsourcing portions of key processes for augmentation by third-party providers. In contrast, corporates in other sectors may lack the internal maturity or resources to benefit fully from managed services. Many are still working to define and standardize their TPRM processes before they can confidently outsource them.

Organizations must ensure that external providers are aligned with internal risk appetites and resilience goals. Leading practices include establishing clear contractual frameworks with service-level agreements (SLAs) and key performance indicators (KPIs) as well as selecting providers that combine technical expertise with a strong customer-centric approach. Effective providers are responsive to the organization's risk profile, focus on high-risk areas, and help streamline assessments to avoid overburdening internal teams.

Leading managed service offerings are increasingly tech-enabled, using AI for high-volume screening and chatbots to accelerate low-risk query resolution. These tools support consistent and efficient service delivery while enhancing the customer experience. Such offerings continue to be enhanced by skilled onshore and offshore subject matter teams who play a key role in delivering end-to-end support where maturity allows.

Strategic recommendations for scaling TPRM through managed services and outsourcing:

Define and mature internal processes before outsourcing: Standardize and document TPRM workflows to ensure readiness for managed service adoption.

Establish strong governance frameworks: Use SLAs and KPIs to maintain oversight and ensure alignment with internal risk appetites and resilience goals. Governance should be embedded in contracts and regularly reviewed.

Select providers with both expertise and customer centricity: Choose partners who understand regulatory expectations, are responsive to your risk profile, and can tailor their services to focus on high-risk areas.

Monitor cultural readiness and change management: Invest in change management to build trust in external providers and the outsourcing model.

Plan for scalability: As TPRM needs evolve, ensure that your managed service model can scale to support broader or more complex risk domains without compromising control or quality.

> "We're seeing a lot of organizations say they use managed services for TPRM, but only a handful are doing it end-to-end. Most are just outsourcing pieces here and there. The real opportunity is bridging that gap—by defining and streamlining your processes and getting the fundamentals right before you scale, you can benefit from faster, more efficient TPRM."

—Roy Waligora
Partner and Global Lead, TPRM
KPMG UK

Technology and AI: Unlocking TPRM maturity and creating value

Technology is reshaping TPRM, with AI and automation offering immense promise — especially in streamlining risk assessments, due diligence, and risk ratings. However, the reality on the ground is messy. AI adoption remains uneven and often fragmented. Most organizations use one to five systems to support TPRM, and integration with other platforms is the top pain point. Automation is typically applied to discrete tasks like due diligence and risk rating, but not across the full lifecycle. The result is a patchwork of disconnected systems that creates more complexity instead of reducing it.

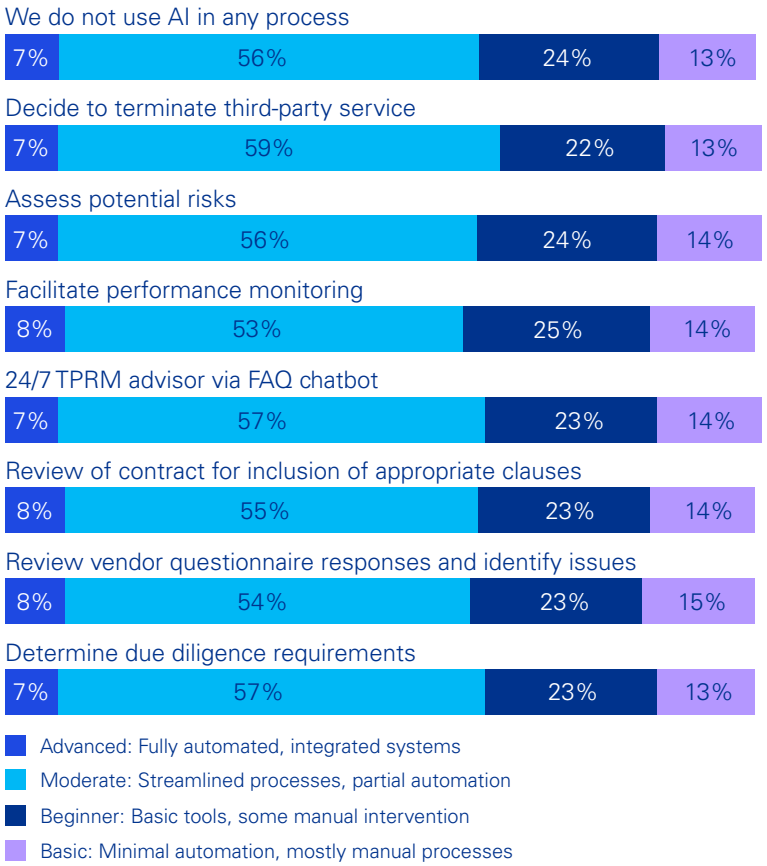
AI adoption is growing, particularly for reporting and data visualization. Yet the effectiveness of AI is also mixed. While 50 percent to 58 percent of respondents claim to use AI, only 22 percent find it "very effective," while 40 percent say it's only "somewhat effective." This effectiveness gap often comes down to trust and orchestration. Organizations that achieve high effectiveness with AI are those that connect disparate processes and have clear ownership over the end-to-end workflow. Siloed, single-step agents are far less effective than a connected, orchestrated process.

The most powerful AI applications combine deep research, purchased insights from databases, and data collected directly from the third party to provide a more complete picture of risk. This allows organizations to assess not just current, real-world events but also to run scenarios, preparing for both "the now and the next." The future of TPRM lies in this end-to-end orchestration, which enables deeper vendor assessments, which gives companies the power not only to react to current events, but also to anticipate what's coming next.

Looking ahead, 39 percent to 47 percent of organizations surveyed expect moderate AI use in core TPRM tasks over the next three years. The opportunity is clear: AI can accelerate end-to-end operations, enhance risk detection, and enable smarter, real-time decision-making. Realizing this potential requires intentional investment, cross-functional collaboration, and a clear roadmap for scaling from pilots to enterprise-wide solutions.

Exhibit 4. Most TPRM programs only use a moderate level of automation, with few benefiting from advanced automation

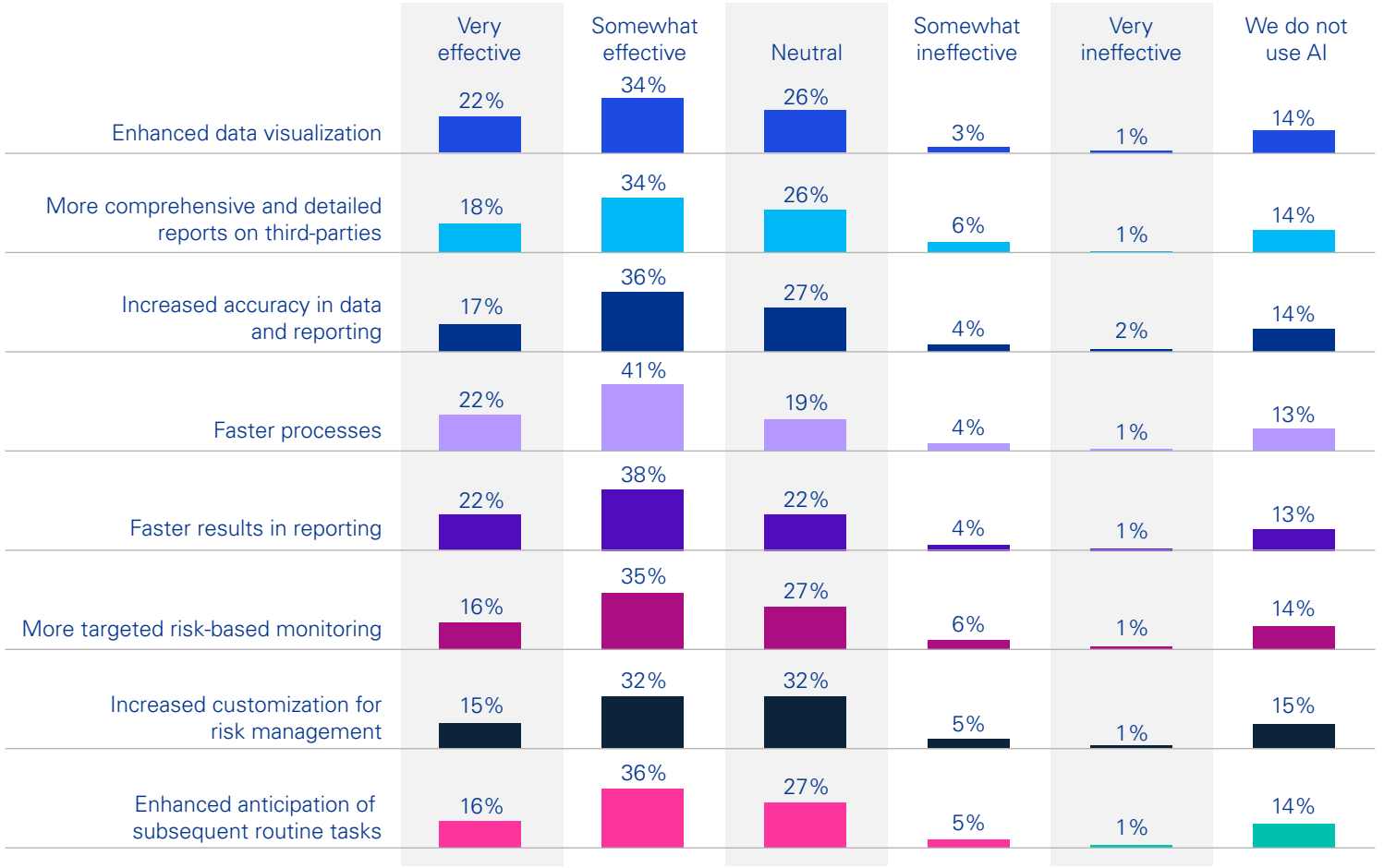
Level of automation of TPRM program and aspects of the TPRM program where automation is leveraged



Notes: (a) Top eight options have been selected for representation purposes, (b) Totals may not equal 100 percent due to rounding
Source: TPRM Survey, 2025

Exhibit 5. AI effectiveness in improving TPRM processes varies

How effective has AI been in improving your TPRM processes?



Notes: (a) "Other" category is not included in the graphical representation, (b) Totals may not equal 100 percent due to rounding
Source: TPRM Survey, 2025

Strategic recommendations for advancing AI and automation in TPRM:

Embed AI within end-to-end workflows: Move beyond isolated use cases and integrate AI across the full TPRM lifecycle — from onboarding to offboarding.

Pair automation with human expertise: Combine AI tools with managed services teams to ensure risk decisions are informed, contextual, and aligned with business goals.

Prioritize system integration: Address platform fragmentation to enable seamless data flow and maximize the value of AI and automation.

Focus on high-impact use cases: Start with areas such as high-volume screening, risk scoring, and chatbot-enabled query resolution to demonstrate quick wins.

Invest in AI readiness: Ensure data quality, governance, and process maturity are in place to support effective AI deployment.

Data quality and confidence: The foundation of trustworthy TPRM

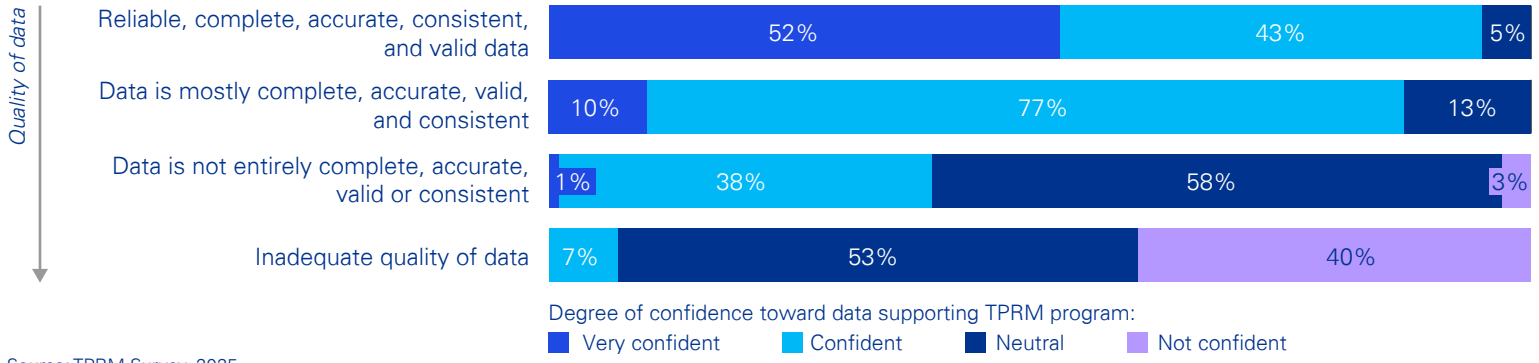
Confidence in the effectiveness of TPRM depends on reliable data. The survey reveals a stark contrast: Leaders with high-quality data are confident in their risk management. Leaders with poor data are not. It's that simple. Consider that among respondents with high-quality data, 52 percent report being "very confident" in their TPRM decisions, whereas 40 percent of respondents with inadequate data quality say they are "not confident."

Improving data quality stands out as an area of significant opportunity for TPRM programs. While 59 percent of respondents say their data is mostly complete, accurate, and consistent, just 17 percent report having the highest level of data quality. Data quality improves with company size, but even large enterprises face challenges in integrating disparate systems and ensuring data integrity.

The disconnect often stems from fragmented systems and inconsistent data practices. For example, procurement systems in different countries may not roll up to a global view, making it difficult to assess third-party risk across geographies. Lack of integration limits visibility into where the highest risks lie in the supply chain. Without a unified view of your third parties, you can't possibly have a unified view of your risk.

Exhibit 5. Confidence in TPRM processes depends on data quality

Quality of the data used in TPRM reporting and confidence in the data supporting the overall TPRM program



Source: TPRM Survey, 2025
Note: Numbers may not equal 100 percent due to rounding

Poor data quality not only creates doubt but also actively undermines your strategic investments. Data quality is a major barrier to effective AI and managed services adoption. Indeed, the survey findings about data quality are at odds with respondents' widespread claims of AI and managed service adoption, suggesting that many organizations are applying these tools only to isolated processes rather than across the full TPRM lifecycle. Without trustworthy data, even the most advanced tools cannot deliver meaningful insights or automation.

Organizations must invest in data governance, standardized reporting, and continuous validation. Yet the challenge can feel overwhelming, especially due to the myriad systems and functional teams involved. Many organizations struggle to know where to begin. A practical approach is to start small, focusing on cleaning and validating data for a subset of vendors that matter most (e.g., critical third parties, specific geographies). Structured, stepwise improvements can yield measurable cost-benefit outcomes and build momentum for broader data governance initiatives.

Strategic recommendations for improving data quality and confidence in TPRM:

Start with critical third parties: Focus initial data cleanup efforts on the most important third parties to drive early wins and demonstrate value.

Adopt a phased approach to data remediation: Break down data quality initiatives into manageable steps that yield cost-benefit at each stage, rather than attempting a full overhaul at once.

Invest in data governance and standardization: Establish clear ownership, consistent definitions, and standardized reporting across business units and geographies.

Integrate procurement and risk systems: Work toward a unified view of third-party data across global operations to improve visibility and risk assessment.

Align data quality efforts with AI and managed service goals: Ensure that foundational data improvements support broader automation and outsourcing strategies.

"Building a foundation of trustworthy data is the most effective way to boost confidence and unlock the full potential of TPRM. The fact that only 17 percent of leaders report having high-quality data highlights a clear path forward. By focusing on data integrity, organizations can get greater value from their technology investments, like AI, and build a truly resilient TPRM program that empowers better, faster decision-making."

— Gavin Rosettenstein
Partner, KPMG Australia

Recommendation roundup: Building a resilient, future-ready TPRM program

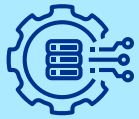
The path to a future-ready TPRM program is not about incremental tweaks; it demands bold, strategic action. To move from a reactive, compliance-driven function to a proactive, value-creating engine of resilience, organizations must embrace a new mindset. The following actions distill the key lessons from the research, offering a clear roadmap to help not only protect your organization but also sharpen its competitive edge:

Focus your firepower.

Shift from broad, inefficient screening to a laser-focused, risk-based model. By concentrating your resources on the small fraction of vendors that pose a genuine threat, you'll gain deeper insights where it matters most and stop wasting effort on low-risk relationships.

Break down the silos.

True resilience is impossible when risk management is a fractured discipline. Integrate your TPRM and ERM functions to create a unified, enterprise-wide view of risk that informs strategic decisions, not just compliance reports.



Treat data as a strategic asset.

Your TPRM program is only as good as the data that fuels it. Invest in data governance to create a single source of truth. Clean, reliable data is the non-negotiable foundation for effective AI, credible reporting, and confident decision-making.

Move beyond "AI theater."

Don't just claim to use AI — deploy it with purpose. Embed automation and intelligent workflows across the entire TPRM lifecycle to accelerate processes, uncover hidden risks, and free up your team for more strategic work.

Look beyond your own backyard.

Your risk exposure doesn't end with your direct vendors. Develop "Nth-party" visibility to understand the risks lurking deeper in your supply chain, enabling you to manage concentration risk and prevent unforeseen disruptions.

Outsource outcomes, not ownership.

Leverage managed services to scale your capabilities and drive efficiency in high-volume activities. However, you must retain firm control over governance and strategy, ensuring that external partners operate as an extension of your risk appetite, not a replacement for it.

How KPMG can help

This report has outlined a playbook for transforming TPRM from a defensive necessity into a strategic advantage. KPMG firms provide the experience, technology, and global scale to help you execute that playbook and win. We work with you to build resilience, drive efficiency, and unlock the strategic value in your third-party relationships. Our global TPRM teams are structured to provide wide-ranging support — combining deep subject-matter experience, advanced technology, and a robust managed services model that sets us apart in the marketplace.

Global team

Our TPRM professionals operate across a network of global delivery centers, with skilled resources available 24/7 in major global hubs. This structure enables us to flex and scale teams to meet client demand, provide multi-time-zone and language support, and deliver consistent, high-quality service across jurisdictions.

Multidisciplinary approach

KPMG firms leverage a multidisciplinary approach, bringing together specialists from risk, procurement, compliance, technology, cyber, and ESG to design, implement, and continuously improve TPRM programs. This cross-functional governance helps ensure that every aspect of your third-party risk program is covered, with effective ownership and accountability.

Modern managed services

The KPMG Managed Service offering for TPRM is an engine of continuous transformation that unites automation, AI, and specialized knowledge on-demand. Our modular, subscription-based service is designed to deliver efficiency gains by leveraging leading-edge technology, automation, and offshore capabilities. Unlike traditional outsourcing, our wide-ranging managed services cover the full TPRM lifecycle — from onboarding and due diligence to continuous monitoring, issue management, and offboarding.

Our TPRM solutions and services deliver measurable value:

- **Efficiency gains:** Reductions in administrative overhead and faster onboarding of third parties, thanks to automation and streamlined processes.
- **Risk reduction:** Our managed services help clients proactively identify, assess, and mitigate risks across the vendor lifecycle, improving overall security posture and compliance.
- **Strategic insights:** Advanced analytics and reporting provide actionable intelligence, enabling better decision-making and continuous improvement.
- **Operational resilience:** By integrating TPRM with ERM and leveraging global resources, KPMG helps organizations build resilience against disruption and regulatory change.

Authors

For more information, contact us:

Alexander Geschonneck

Partner, Global Forensic Leader
KPMG Germany
ageschonneck@kpmg.com

Alexander is the Global Lead for KPMG Forensic. Alexander advises companies, banks, and public organizations on investigations, anti-money laundering, and anti-fraud and anti-corruption measures. In addition, he coordinates KPMG's global Forensic practices to support clients in responding to the threat of financial crime.

Joey Gyengo

Principal, US Third Party Risk Management Lead,
KPMG US
jgyengo@kpmg.com

Joey is an Atlanta-based principal in KPMG's Consulting practice and the US Enterprise Risk Management (ERM) and Third Party Risk Management (TPRM) leader. His 20-plus years of experience include a deep background in enterprise risk and resilience; governance, risk, and compliance (GRC); internal audit; and internal controls. Joey advises boards and senior leadership on risk strategy, risk governance, and risk management.

Roy Waligora

Partner and Global Lead, TPRM
KPMG UK
roy.waligora@kpmg.co.uk

Roy is a Forensic partner based in London. He leads on Global Third Party Risk Management, supporting our global teams and clients to respond to the challenge of managing third parties effectively enabled by technology. Roy also has over 25 years of cross-border due diligence and investigations experience.

We would like to thank our contributors:

Laura Bubeck, Jilane Khakkhar, Lauren J. Polana, Matthew P. Miller, Rohit Nag, Tara Nelson, Kathleen Nichols, Rama Ramaswami, Rishab Sengupta, Chandra Shekhar, Constance Thaete, and Anshita Tripathi.

Connect with our global working group

UK and Global

Roy Waligora
Partner and Global Lead, TPRM
KPMG UK
roy.waligora@kpmg.co.uk

Helena Bartles
Director, Forensic
helena.bartles@kpmg.co.uk

US

Joey Gyengo
Principal, US Third Party Risk Management Lead
jgyengo@kpmg.com

Daniel W. Click
Partner, Advisory
dclick@kpmg.com

Diana Keele
Managing Director,
Risk Services
dkeele@kpmg.com

Canada

Sonu Sikand
Partner, Info Tech Risk Services
sonusikand@kpmg.ca

Peter W. Armstrong
Partner, Forensic
pearmstrong@kpmg.ca

India

Vipul Jain
Partner, India Lead, Non-Cyber Third-Party Risk Management
vipuljain@kpmg.com

Srijit Menon
Partner, KPMG India Global Lead, Third Party Security
srijitmenon@kpmg.com

Maneesha Garg
Partner and Head,
Managed Services
maneesha@kpmg.com

Netherlands

Hokkie Blogg
Partner, Cyber Strategy & Risk
blogg.hokkie@kpmg.nl

Belgium

Jens Moerman
Director, Forensic
jensmoerman@kpmg.com

Germany

Verena Hinze
Audit — Regulatory Advisory
vhinze@kpmg.com

France

Caroline Albarel
Partner, Advisory
calbarel@kpmg.fr

Italy

Valerio Falcicchio
Partner, Advisory
valeriofalcicchio@kpmg.it

Daniele Ianniello
Partner, Advisory
dianniello@kpmg.it

Japan and ASPAC

Mariko Yamada
Director, Forensic
mariko.yamada@jp.kpmg.com

Australia and South ASPAC

Gavin Rosettenstein
Partner, KPMG Australia
gavin1@kpmg.com.au

Middle East

Nicholas Cameron
Partner, KPMG United Arab Emirates
nicholascameron@kpmg.com

Related insights

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

Please visit us: **kpmg.com**