KPMG

Achieving resilience in third-party risk management

Global third-party risk management survey

—

2026

As organizations become increasingly dependent on contractors, suppliers, service providers, and technology partners, Third Party Risk Management (TPRM) is emerging as one of the key components of operational resilience and corporate governance.

Digitalization, the growing complexity of global supply chains, rising regulatory requirements, and escalating cyber threats have significantly transformed the TPRM landscape. Organizations are now expected not only to identify and assess risks but also to continuously monitor them, respond promptly, and adapt throughout the entire lifecycle of third-party relationships. At the same time, many companies note that their resources remain disproportionately focused on assessing low-risk counterparties, while the most significant risks do not always receive sufficient attention.

The rapid digital transformation, expansion of global supply chains, stricter regulatory requirements, and increased cyber threats have profoundly changed the TPRM environment. Today, organizations are expected not only to detect and evaluate risks but also to maintain ongoing monitoring, timely response, and adaptation to emerging challenges throughout the full lifecycle of engagement with third parties. Nevertheless, most clients report that they do not always manage to do this effectively, as their resources are often overloaded with assessing low-risk third parties instead of focusing on partners that pose truly significant risks.

.

Against this backdrop, our survey explores the latest trends, practices, and challenges in Third Party Risk Management. It provides insights into how organizations are transforming their TPRM systems, implementing new technologies, engaging external providers, integrating risk management functions, and responding to regulatory and operational requirements. The report also offers strategic recommendations for managing third-party risks, with a focus on enhancing resilience and creating additional value.

Alexander Geschonneck
Global Lead, Forensic

Roy Waligora
Global Lead, Third Party Risk Management

Effective third-party risk management is becoming both critically important and increasingly complex in today's interconnected business environment.

KPMG's global TPRM study provides a practical "roadmap" for shifting from reactive, fragmented approaches to a proactive, scalable, and future-oriented model of third-party risk management. Regulatory and cyber risks remain in focus as the most significant and urgent threats.

The study highlights substantial potential for:

- deepening the integration of TPRM with ERM,
- scaling operating models,
- more meaningful use of AI,
- improving data quality and reliability.

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.

Our 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 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.

Executive summary

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

Despite the fact that only 53% of Third Party Risk Management (TPRM) programs are integrated with Enterprise Risk Management (ERM) to some extent, and only 71% are fully integrated, there remains significant potential to establish a unified, enterprise-wide view of risks.

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.

Hotline / Whistleblowing

The hotline is an important tool within the compliance and risk management system, providing a secure and confidential channel for reporting potential violations, including fraud, corruption, conflicts of interest, and breaches of business ethics.

Integrating the hotline into compliance and risk management processes enables organizations to identify potential violations in a timely manner, strengthen internal control systems, and obtain an additional source of information for risk monitoring, including risks related to third parties (TPRM).

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 cuts through the noise, distilling our 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

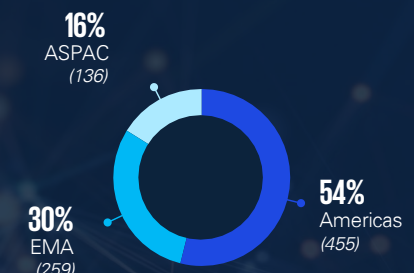
In 2025, KPMG conducted an online survey of 851 respondents across various industries and regions (Americas, Europe, Asia-Pacific).

The study involved executives and professionals directly engaged in third-party risk management, enterprise risk management, compliance, cybersecurity, and operational functions.

The assessment covered:
- the maturity of TPRM programs,
- systems and tools in use,
- approaches to risk assessment and monitoring,
- third-party lifecycle management,
- levels of resilience, data quality, and the use of technology.

Respondent overview

Organization's region



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%

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)*

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

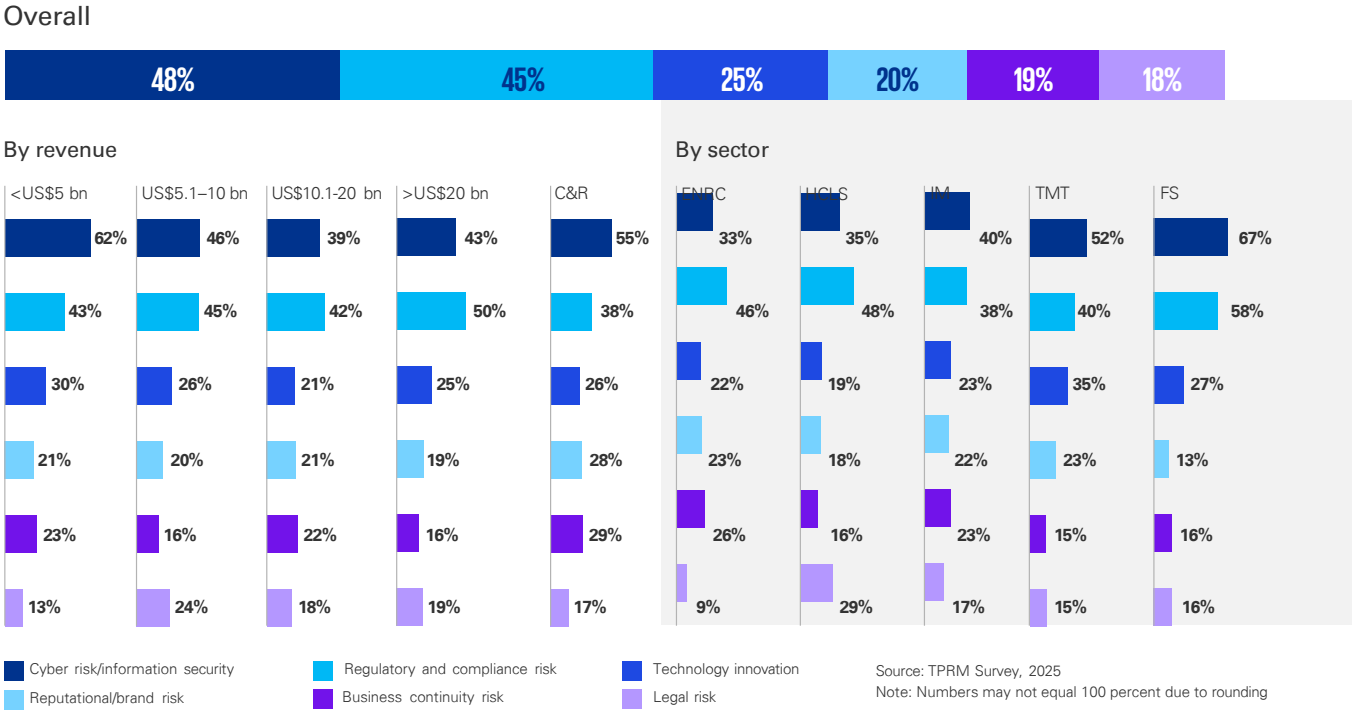
Compliance and cybersecurity: Twin pillars of TPRM strategy

Compliance risks and cyber risks remain the two dominant pillars of TPRM strategy. For most organizations, the current approach is predominantly defensive, reflecting justified concerns about how quickly third-party vulnerabilities can spread across the entire enterprise.

Investment priorities align with these concerns, but they often do not result in the development of a comprehensive and mature third-party risk management framework.

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

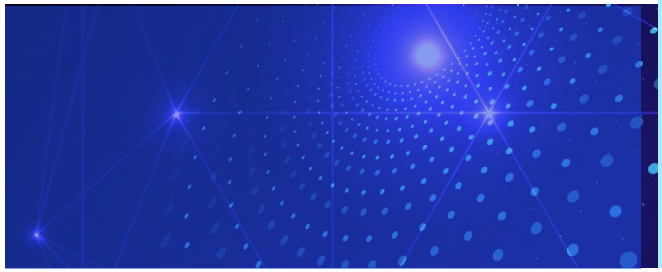
Sector-specific nuances also impact drivers of TPRM strategy
as well as spending priorities. For example, financial services firms are driven by stringent regulatory mandates, while life sciences organizations face complex compliance demands tied to diverse third-party relationships. Meanwhile, manufacturers 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]

In our extensive experience helping design and manage TPRM programs for clients, we see companies with tens of thousands of vendors trying to screen everyone, when only a smaller fraction—perhaps 10 to 20 percent—pose higher risks that warrant deeper investigation. This is a massive opportunity to refocus effort where it matters 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:

The growth and increasing complexity of third-party ecosystems are leading to an exponential rise in the number of risks. In many organizations, tens of thousands of suppliers undergo formal screening, while only 10–20% of them actually pose elevated risk and require in-depth analysis.

Developing visibility into Nth-party risks requires particular attention, including concentration risks and hidden dependencies on specific regions or suppliers.

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

Regulatory requirements and scrutiny are rising

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

Kazakhstan

- Law "On Informatization"
- Law "On Personal Data and Its Protection"
- NBK Rules No. 48 and 188
- AFSA Guidelines for the Risk Management Policy
- AIFC General Rules

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 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

United Kingdom

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

India

- Financial Services - RBI Guidance On Management Third Party Risk

Australia

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

Integration challenges: Despite the declared integration, TPRM and ERM in many organizations still operate within different managerial and operational logics

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.

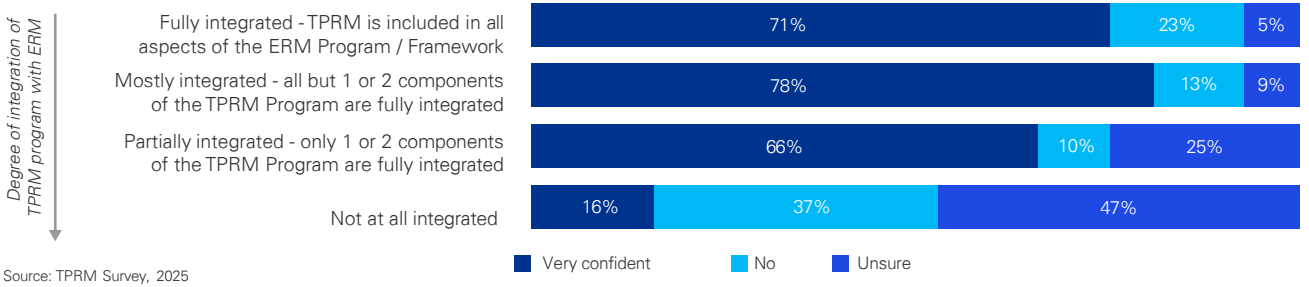
In practice, 'partial integration' often comes down to transferring aggregated TPRM data into ERM reporting without establishing a deep linkage between processes, systems, and decision-making. Distributed responsibility across functions (procurement, information security, compliance, operations) further complicates the creation of a unified view of risks. 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.

"In the context of the growing number of incidents related to service providers and increasing regulatory scrutiny, third-party risk management is becoming critically important for companies in Kazakhstan. Organizations need to place greater emphasis on assessing risks associated with their contractors and partners in order to ensure resilience and compliance with regulatory requirements."

Konstantin Aushev
Partner, Head of
Technology Practice
KPMG Caucasus and Central Asia

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.

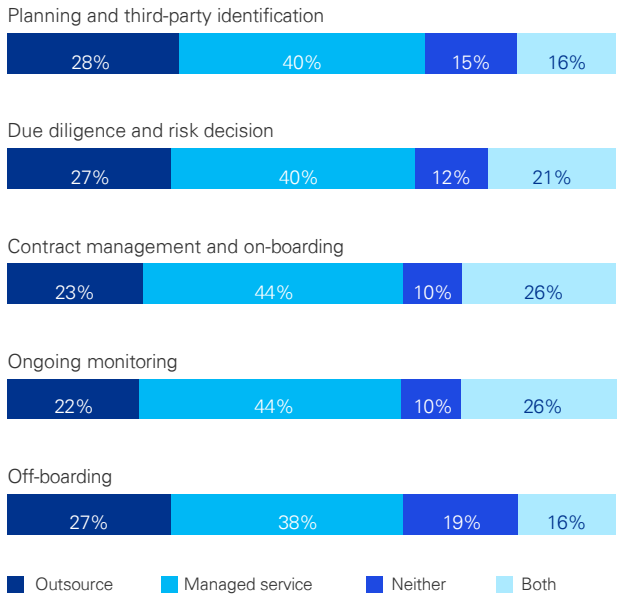
Most organizations use outsourcing, co-sourcing, or managed services for individual stages of TPRM, primarily for high-volume and labor-intensive processes.

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: Clear SLAs and KPIs, as well as the organization's ability to manage the provider as an extension of its own risk-management strategy, become a key success factor 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

Artificial intelligence and automation offer significant potential to improve the efficiency of TPRM; however,
in practice, implementation is 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.

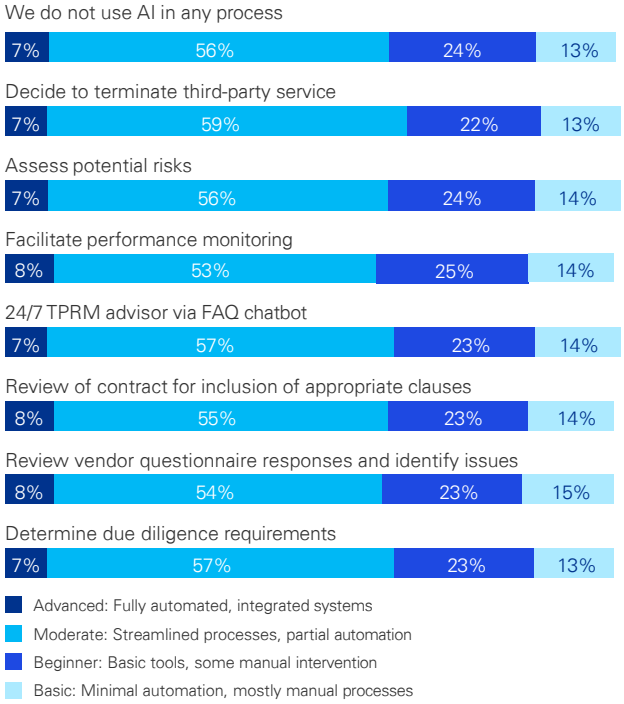
AI adoption is growing, particularly for reporting and data visualization. Yet the effectiveness of AI is also mixed. While 50 percent to 58 percent of respondents claim to use AI, only 22 percent find it "very effective," while 40 percent say it's only "somewhat effective." This effectiveness gap often comes down to trust and orchestration. Organizations that achieve the greatest value from AI focus not on individual use cases, but on orchestrating end-to-end processes, clearly defining responsibilities, and ensuring the quality of underlying data. 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 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

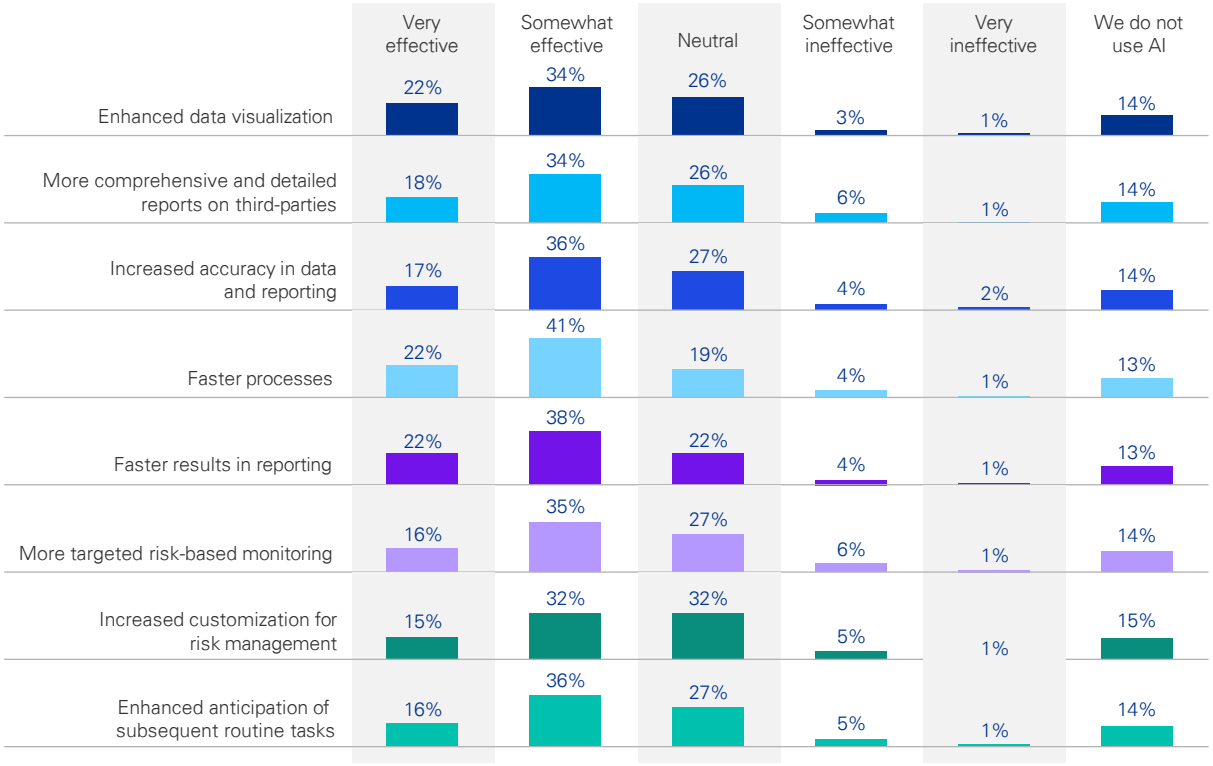


Notes: (a) Top eight options have been selected for representation purposes, (b) Totals may not equal 100 percent due to rounding

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

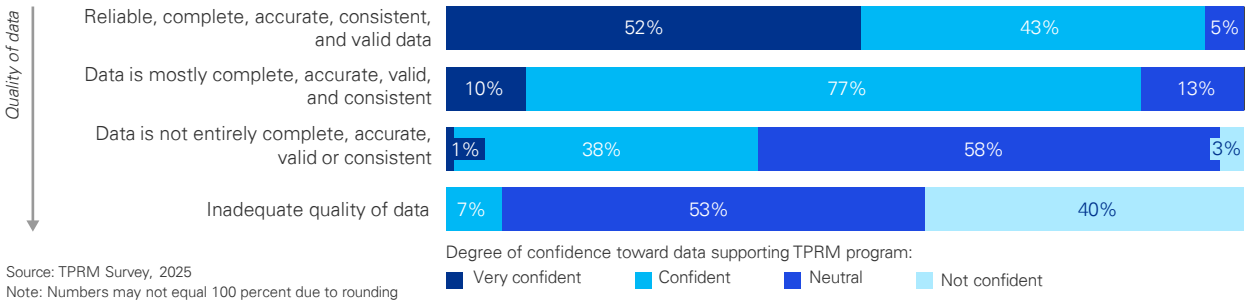
Confidence in the effectiveness of TPRM depends on reliable data. Our survey reveals a stark contrast: Leaders with high-quality data are confident in their risk management. Leaders with poor data are not. It's that simple. Consider that among respondents with high-quality data, 52 percent report being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

Data quality is the foundation of a reliable TPRM program. The study reveals a direct correlation between data quality and leadership's confidence in decision-making.

System fragmentation, inconsistent taxonomies, and the absence of a single source of truth significantly limit the potential for analytics, automation, and integration with ERM.

Exhibit 6. 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 our research, offering a clear roadmap to not only protect your organization but also sharpen its competitive edge:

Focus resources on the risks that truly matter, rather than attempting a formal coverage of the entire ecosystem

Eliminate organizational and technological gaps between TPRM and ERM

Treat data as a strategic asset rather than a byproduct of processes

Shift from 'AI theater' to intentional automation of end-to-end processes

Expand the risk-management perimeter beyond direct suppliers

Outsource the outcomes, but not the responsibility for risk

How KPMG can help

This report has outlined a playbook for transforming TPRM from a defensive necessity into a strategic advantage. KPMG provides 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 team is 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 leverages 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 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:

Konstantin Aushev

Partner, Head of Technology practice
KPMG Caucasus and Central Asia
E: kaushev@kpmg.kz

Gabit Musrepov

Partner, Head of GRCS & ORS Practice
KPMG Caucasus and Central Asia
E: GMusrepov@kpmg.kz

Damir Yerkin

Director of Technology Practice
KPMG Caucasus and Centra Asia
E: damiryerkin@kpmg.com

Roman Kim

Associate Director of GRCS & ORS Practice
KPMG Caucasus and Central Asia
E: romankim@kpmg.kz