Global TPRM survey 2026 Report

Technology, Media, Telecommunications (TMT)

The 2025 Global Third-Party Risk Management (TPRM) Survey gathered input from 851 senior leaders worldwide, across 16 countries, including 164 participants from the technology, media, and telecommunications (TMT) sector. Our report provides a comprehensive view of third-party risk practices across industries and regions. Within TMT, the dataset reflects perspectives from organizations spanning technology, media, and telecommunications, enabling a representative assessment of how TMT enterprises are advancing their third-party risk management capabilities.

Cyber risk management, regulatory compliance, and data governance are key drivers of third-party risk programs. Despite these priorities, organizations struggle with integration, regulatory demands, and monitoring performance. Investments in technology, cybersecurity, and risk assessment signal a shift toward tech-enabled strategies for resilience and efficiency.

Key drivers of TPRM activity in organizations

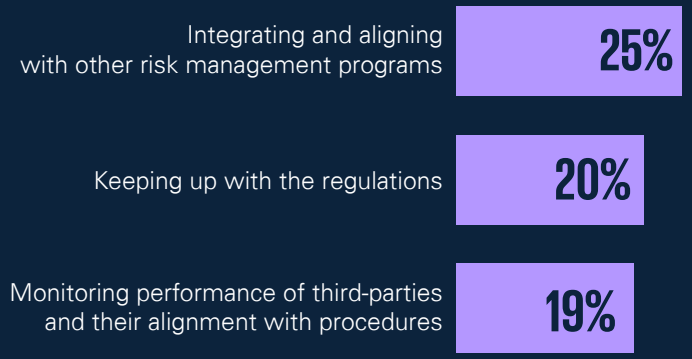
TMT organizations are motivated by the need to address cyber threats, comply with evolving regulations, and safeguard data privacy. These priorities reflect the sector's exposure to digital risks and regulatory scrutiny, as highlighted in our report's call for proactive, tailored risk management.

39% Managing cyber risk

36% Ensuring compliance with regulations

34% Data governance and privacy

Top 3 challenges of TPRM



TMT organizations face persistent challenges integrating TPRM with other risk management functions, keeping pace with regulations, and monitoring third-party performance. These hurdles reflect the report's observation that fragmented ownership and evolving compliance demands complicate efforts to build a unified, resilient risk management strategy.

Key TPRM spending priorities for the next 12 months

Investment is focused on advanced technology, cybersecurity measures, and robust risk assessment processes. This approach aligns with the report's recommendation for leveraging tech-enabled solutions to strengthen third-party risk management and build resilience.

67% Technology and tools for TPRM

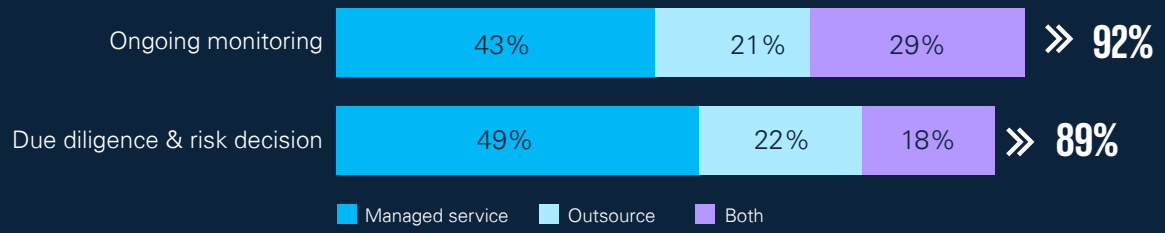
60% Cybersecurity and data protection measures

45% Risk assessment and due diligence procedures

TMT organizations increasingly rely on managed services and outsourcing for ongoing monitoring and due diligence, reflecting a shift toward scalable external support while maintaining strong governance. Efficient onboarding is prioritized for critical third parties using risk-based approaches, but operational challenges such as security reviews, risk management involvement, and background checks often slow the process. These factors underscore the need for streamlined workflows and cross-functional collaboration to accelerate onboarding and strengthen risk oversight.

TPRM areas utilizing managed services and/or outsourcing

Most TMT organizations rely on external partners for ongoing monitoring and due diligence, adopting a mix of managed services and outsourcing models. The report notes that scalable external support is increasingly important, though organizations must maintain strong governance and integration.



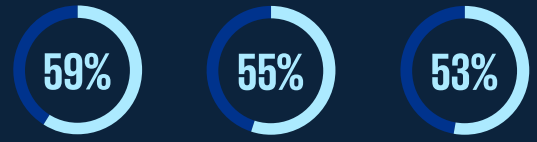
Average time to onboard selected third-party by risk level

Organizations prioritize efficient onboarding for critical third parties, using risk-based approaches to allocate resources where they have the greatest impact. The report emphasizes the value of focusing efforts on high-risk relationships to accelerate onboarding and enhance risk oversight.

Level of importance	0-30 days	30-60 days
Critical	60%	13%
High	51%	32%
Moderate	41%	53%

Key factors affecting third-party onboarding duration

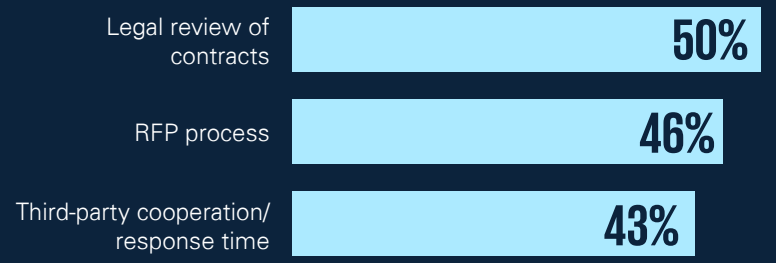
Operational challenges such as information security processes, risk management involvement, and thorough background checks can slow onboarding. The report advocates for streamlined workflows and collaboration across functions to reduce bottlenecks and improve efficiency.



Delays in third-party assessments often stem from legal reviews, procurement steps, and vendor responsiveness, highlighting the need for integrated risk processes. Cybersecurity, compliance, and technology innovation are rising priorities, while recent incidents have caused reputational, financial, and supply chain impacts. Integration between TPRM and Enterprise Risk Management (ERM) remains limited, underscoring the need for unified governance and shared controls.

Key factors affecting the timeline for third-party assessment through contract signing

Legal review, procurement processes, and third-party responsiveness are common sources of delay in contract signing and assessment. Integrating risk management into these processes is essential for strategic, timely decision-making, as recommended in our report.



Emerging risks gaining importance in TPRM over recent years

Cyber/information security, regulatory compliance, and technology innovation are increasingly prioritized as emerging risks. The report underscores the need for TMT organizations to anticipate new threats and adapt their risk management frameworks to address the evolving landscape.

52% Cyber risk/information security

40% Regulatory and compliance risk

35% Technology innovation

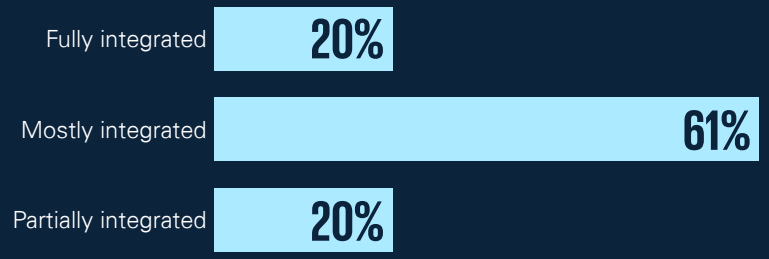
Organizations' experience with third-party issues in the last three years

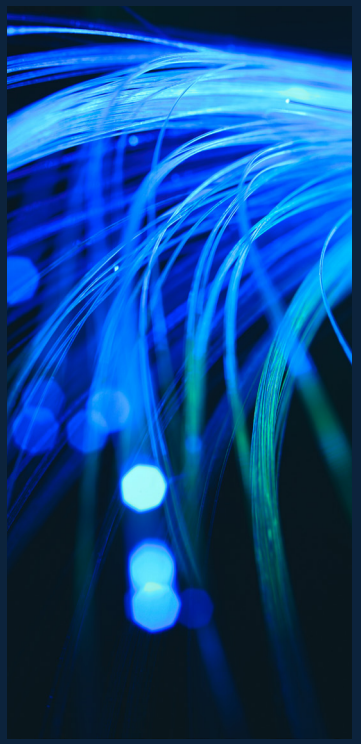
A significant portion of TMT organizations have avoided major third-party incidents, but those that did experience issues most faced reputational damage, monetary loss, or supply chain disruption. Our report highlights the importance of proactive measures and robust incident response to mitigate these risks and protect organizational value.

	1-2 times	3-5 times
Significant reputational damage	28%	6%
Significant monetary loss	32%	24%
Significant supply chain disruption	28%	10%

Integration level between TPRM and ERM programs

Most TMT organizations report partial or moderate integration between TPRM and ERM, with only a minority achieving full alignment. This mirrors the survey's finding that integration remains a work in progress, and emphasizes the need for shared controls, unified assessments, and cross-functional governance.

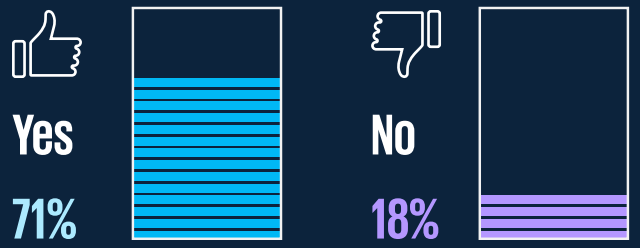




Most organizations plan to deepen integration between third-party and ERM, aiming for a more unified approach. To strengthen resilience, they focus on post-incident reviews, contingency planning, and predefined response strategies. Confidence in TPRM data remains moderate, with reliance on multiple systems creating complexity and highlighting the need for streamlined platforms and stronger data governance.

Plans for further TPRM and ERM integration in the next three years

A majority plan to deepen integration between third-party and enterprise risk management, aiming for a more cohesive and strategic approach to risk oversight.

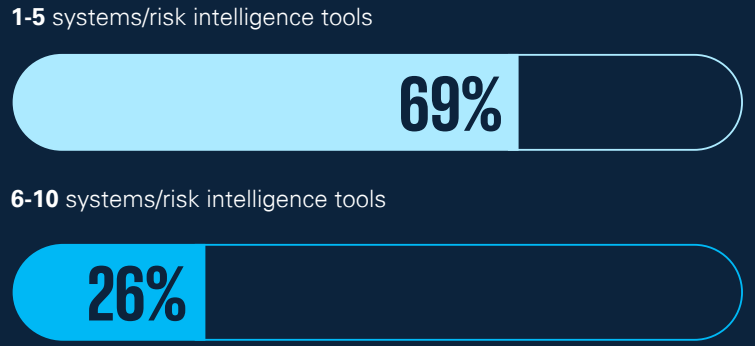


Confidence in data quality and reliability that support TPRM programs

Most organizations express moderate confidence in their TPRM data, but few report high confidence. This reflects the report's emphasis on data quality as a foundational challenge, where fragmented systems and inconsistent practices undermine trust and limit effective risk management.

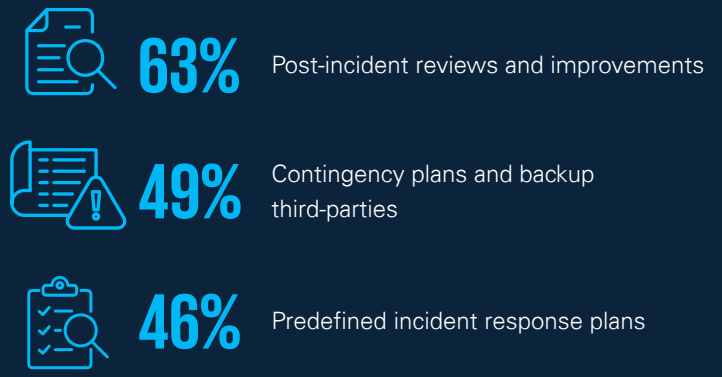
Number of systems/risk intelligence tools supporting the TPRM program

The majority rely on multiple systems or risk intelligence tools, often leading to complexity and integration issues. The report highlights this fragmentation as a major barrier to efficiency and calls for unified platforms to enable seamless data flow and holistic risk oversight.



Strategies for managing third-party incidents and disruptions

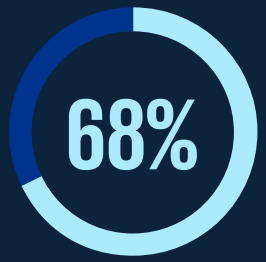
Organizations are prioritizing post-incident reviews, contingency planning, and predefined response strategies to manage third-party disruptions, embedding these practices into broader risk frameworks to strengthen resilience and enable faster recovery.



TMT organizations struggle with system integration, maintenance costs, and data reliability, limiting efficiency and risk insight. Automation remains partial and focused on early tasks, while AI offers faster processes and reporting but requires integrated workflows and governance to deliver full value.

Degree of automation maturity in TPRM

Automation is present but remains largely partial, with streamlined processes applied to select tasks rather than across the full lifecycle. Many organizations adopt automation in isolated steps, which creates inefficiencies and limits the potential for end-to-end orchestration.



Respondents reported having a Moderate: Streamlined processes, partial automation level of automation in their TPRM programs

Automation deployment across stages of the TPRM lifecycle

Automation is concentrated in early lifecycle stages such as due diligence and risk rating, while broader integration remains limited. Our report's recommendation is to embed automation across the entire TPRM process to accelerate workflows and improve resilience

41% Determine due diligence requirements

39% Assign inherent risk rating

37% Document risk, risk rating, recommendation for an issue

Most challenging pain points with existing TPRM technology

46%
Integration with other systems

32%
Cost of maintenance and upgrade

31%
Data accuracy and reliability

Integration gaps, maintenance costs, and data reliability are persistent pain points for TMT organizations. These challenges reinforce out report's guidance to prioritize system integration and data governance as prerequisites for scaling automation and achieving meaningful risk insights.

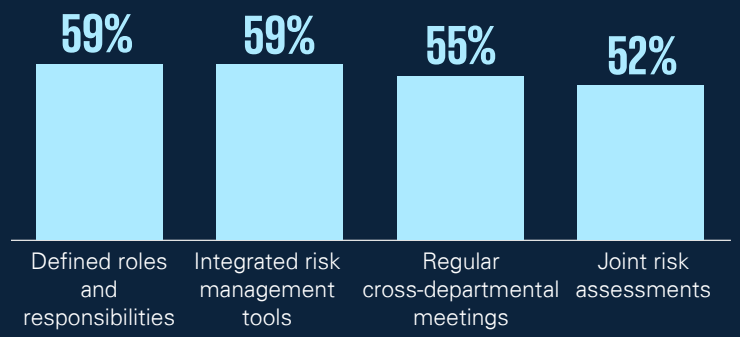
Effectiveness of AI in enhancing TPRM processes

AI delivers benefits like faster processes and improved reporting, but effectiveness varies widely. The report notes that success depends on pairing AI with strong governance and integrated workflows, rather than isolated use cases that create a patchwork of tools.

Organizations are aligning third-party risk management with resilience by defining roles, integrating frameworks, and fostering collaboration. Compliance, reduced downtime, and faster incident response drive adoption of AI tools like monitoring, predictive analytics, and machine learning. Plans focus on implementing new technologies, piloting solutions, and training staff to embed automation for efficiency and resilience.

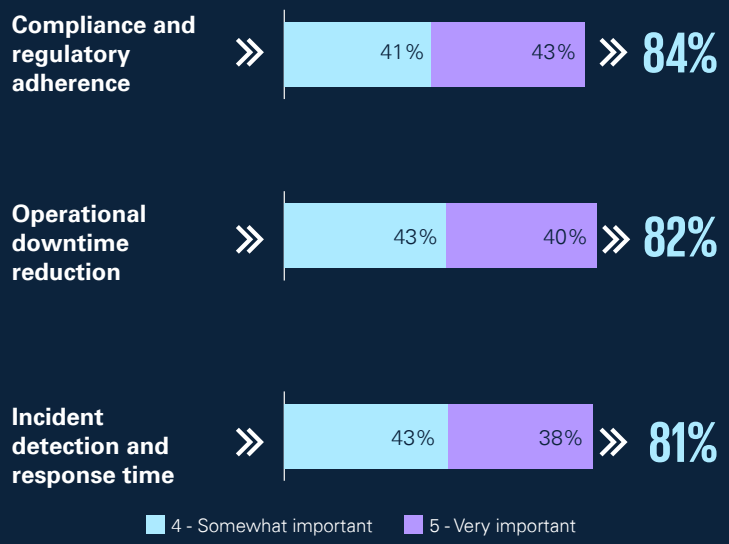
Strategies for ensuring alignment between TPRM and operational resilience objectives

Organizations are emphasizing clear roles, integrated risk frameworks, and cross-department collaboration to strengthen alignment between third-party risk management and resilience goals. These practices help break down silos and create a unified approach to managing disruptions.



Key indicators of success for TPRM and operational resilience integration through AI

Compliance adherence, minimizing downtime, and faster incident response are viewed as critical measures of success. This reflects the growing need for AI-driven solutions that not only improve efficiency but also enhance resilience against regulatory and operational risks.



Note: Percentages may not total 100%, as respondents could select multiple options. Data reflects "somewhat important" and "very important" responses.

Key AI/automation technologies integrating TPRM with operational resilience

AI-driven monitoring, predictive analytics, and machine learning are leading technologies used to connect risk management with resilience objectives. These tools enable proactive identification of vulnerabilities and support smarter, real-time decision-making.

67% AI-driven monitoring and alerting systems

59% Predictive analytics

48% Machine learning algorithms

Plans for advancing TPRM and operational resilience synergy through AI

Organizations plan to implement new AI technologies, run pilot programs, and invest in training to scale automation effectively. These steps signal a shift toward embedding AI across the lifecycle to drive efficiency and strengthen resilience strategies.

54% Implementing new AI technologies

52% Conducting pilot projects or proofs of concept

51% Training staff on AI and automation

Contact us

Joey Gyengo
Principal, US Third Party Risk Management Leader
KPMG LLP
E: jgyengo@kpmg.com

Lisa Rawls
US TMT Industry Leader for Risk Services
KPMG LLP
E: lisarawls@kpmg.com

Filippo Puglisi-Alibrandi
Principal, Risk Services
KPMG LLP
E: fpuglisialibrandi@kpmg.com

Matt Tobey
Principal, Risk Services
KPMG LLP
E: mtobey@kpmg.com

Daniel W. Click
Partner, Risk Services
KPMG LLP
E: dclick@kpmg.com

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**