2026 KPMG Global Third-Party Risk Management Survey

Financial Services

The 2026 KPMG Global Third-Party Risk Management (TPRM) Survey gathered input from 851 senior leaders across 16 countries worldwide, including 165 participants from the financial services sector. Our report provides a comprehensive view of third-party risk practices across industries and regions. Within financial services, the dataset captures viewpoints from banking, capital markets, insurance, and other financial institutions, enabling a representative assessment of how FS organizations are advancing their third-party risk management capabilities.

Organizations in financial services are focused on compliance, cyber risk, and data governance as key elements of third-party risk management (TPRM). However, this approach is hindered by fragmented systems, monitoring challenges, and regulatory complexities. Cybersecurity, compliance, and technology tools are expected to drive TPRM investment priorities over the next 12 months.

Key drivers of TPRM activity in organizations

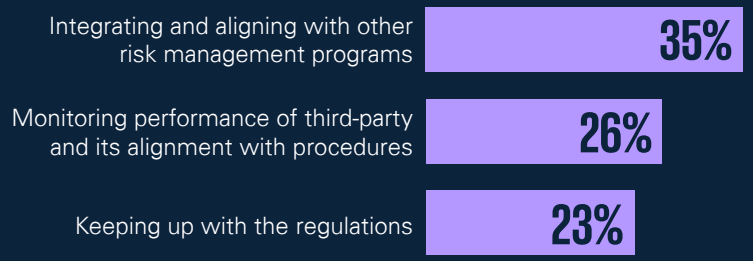
Organizations are prioritizing TPRM due to regulatory pressures, heightened risk exposure, and the need for operational resilience. These drivers reflect a shift toward proactive risk management and stronger governance frameworks.

60%
Ensuring compliance with regulations

51%
Managing cyber risk

38%
Data governance and privacy

Top 3 challenges of TPRM



The most cited challenges—fragmented integration, monitoring third-party performance, and regulatory complexity—reflect the need for unified, proactive risk management. These obstacles hinder organizations from achieving holistic oversight and resilience.

Key TPRM spending priorities for the next 12 months

Regulatory compliance, cyber risk, and data governance continue to shape the priorities and investments in TPRM for the next 12 months. Organizations are channeling resources into cybersecurity, technology enablement, and audit readiness to address these drivers, reflecting a shift toward more proactive and resilient risk management.

65%
Cybersecurity and data protection measures

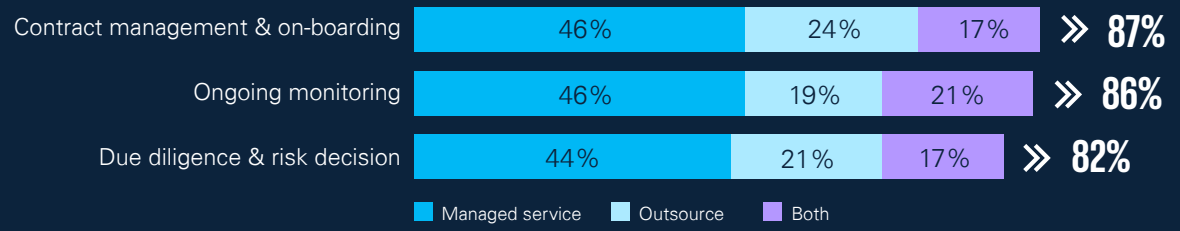
54%
Technology and tools for TPRM

52%
Regulatory compliance and audits

Organizations in financial services are adopting managed services and outsourcing, enabling them to scale their risk programs and respond quickly to changing demands. Prioritizing information security and thorough assessments ensures that new third parties are vetted effectively, while efficient onboarding and contract review processes help maintain business momentum without compromising risk standards.

TPRM areas utilizing managed services and/or outsourcing

Managed services and outsourcing have become standard practices for contract management, onboarding, monitoring, and due diligence, enabling organizations to efficiently handle large volumes of third parties. However, most still rely on partial outsourcing rather than full end-to-end models, underscoring the importance of maturing internal processes and maintaining strong governance frameworks.



Average time to onboard selected third-party by risk level

Onboarding timelines for third parties typically fall within 0–60 days, with critical vendors prioritized for faster integration. This approach supports risk-based screening, ensuring that resources are concentrated where they matter most.

Level of importance	0-30 days	30-60 days
Critical	60%	19%
High	42%	39%
Moderate	39%	38%

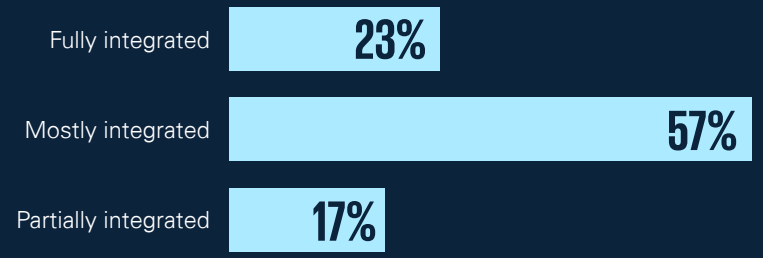
Key factors affecting third-party onboarding duration

Information security process time, risk management involvement, and third-party background checks are the primary factors influencing onboarding duration. Effective cross-functional collaboration and integrated governance help organizations accelerate onboarding while maintaining robust controls.

Organizations are prioritizing system integration, adopting proactive strategies, and investing in advanced technology, such that these organizations can bolster their resilience and mitigate exposure to emerging risks.

Integration level between TPRM and ERM programs

Partial or moderate integration is common, limiting strategic oversight and unified decision-making. Investing in shared controls and joint governance is essential for holistic risk management.



Emerging risks gaining importance in TPRM over recent years

Cyber risk and regulatory compliance are top concerns in financial services, with technology innovation also rising in importance. Addressing these risks requires investment in advanced tools and continuous adaptation.

68% Cyber risk/information security

57% Regulatory and compliance risk

26% Technology innovation

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

Frequent reputational damage, monetary loss, and supply chain disruptions from third-party incidents emphasize the importance of proactive risk mitigation and robust incident response, aligning with the call for future-ready approaches.

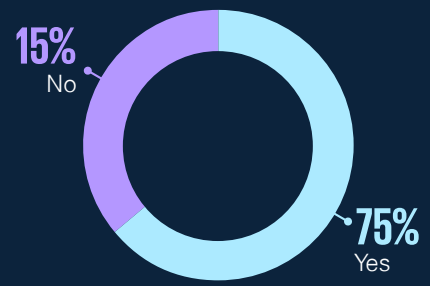
	1-2 times	3-5 times
Significant reputational damage	28%	6%
Significant monetary loss	32%	24%
Significant supply chain disruption	28%	10%

Strategies for managing third-party incidents and disruptions

Post-incident reviews, contingency planning, and financial incentives or penalties for third parties are key approaches to bolster resilience and enhance risk management.

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

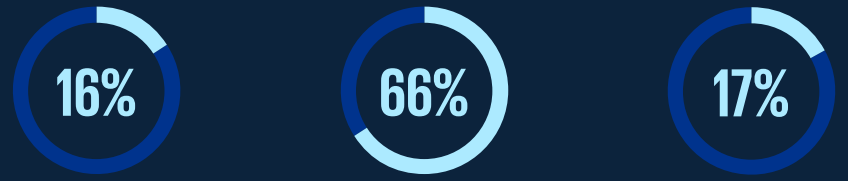
A majority plan to deepen integration between third-party and enterprise risk management, aiming for a more cohesive and strategic approach to risk oversight.



Reliable data integration and robust security measures are crucial for effective third-party risk management. Overcoming fragmentation through integration with other systems, improving security and data protection measures, and enhancing data accuracy and reliability will foster trust and efficiency in risk management technology.

Confidence in data quality and reliability that support TPRM programs

Most organizations express confidence in their data, but only a small fraction rate it as very high quality. This gap highlights the ongoing challenge of achieving truly reliable data to support effective risk management.

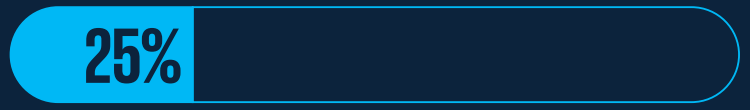


Number of systems/risk intelligence tools supporting the TPRM program

The majority of respondents rely on a limited number of systems or tools, which can lead to fragmented processes and integration challenges. Streamlining and integrating these systems is essential for a unified approach to third-party risk.

1-5 systems/risk intelligence tools

6-10 systems/risk intelligence tools



Most challenging pain points with existing TPRM technology

Integration with other systems, security and data protection, and data accuracy are the top pain points. Addressing these issues is critical for improving efficiency and trust in risk management technology.

44% Integration with other systems

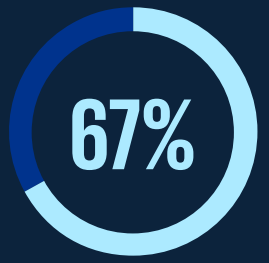
37% Security and data protection

32% Data accuracy and reliability

Advanced automation is foundational for effective third-party risk management. Investing in AI/automation technologies will accelerate processes, improve reporting, and enable smarter decision-making.

Degree of automation maturity in TPRM

Most organizations report moderate automation, with streamlined processes but only partial automation across the lifecycle. Advancing automation can accelerate risk assessments and reporting.



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

Automation deployment across stages of the TPRM lifecycle

39%

Document risk, risk rating, recommendation for an issue

37%

Review vendor questionnaire responses and identify issues

37%

Assign inherent risk rating

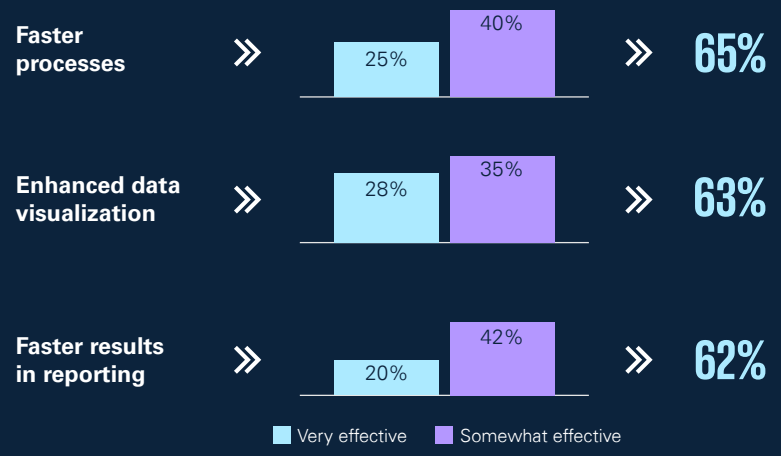
34%

Predicting/generating inherent risk assessment

Automation is most commonly used for document risk rating, reviewing questionnaires, and assigning risk ratings, while predictive assessments are less widespread. Expanding automation to more stages can enhance consistency and speed.

Effectiveness of AI in enhancing TPRM processes

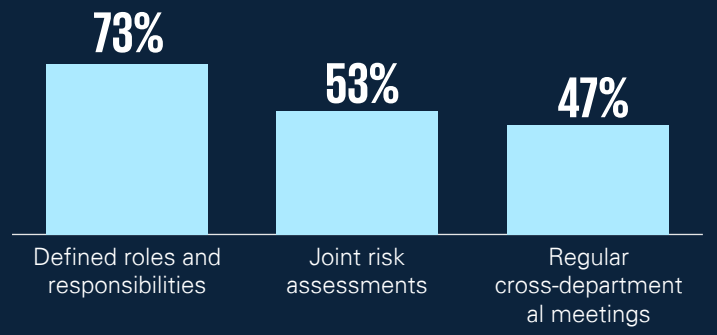
AI is seen as somewhat effective in speeding up processes, improving data visualization, and accelerating reporting, but very high effectiveness remains limited. Continued investment in AI and data quality will be key to unlocking greater value.



Integrating third-party risk management with operational resilience requires collaboration, advanced technology, and a focus on key performance indicators. Organizations investing in AI and cross-functional strategies are better positioned to manage disruptions and regulatory demands.

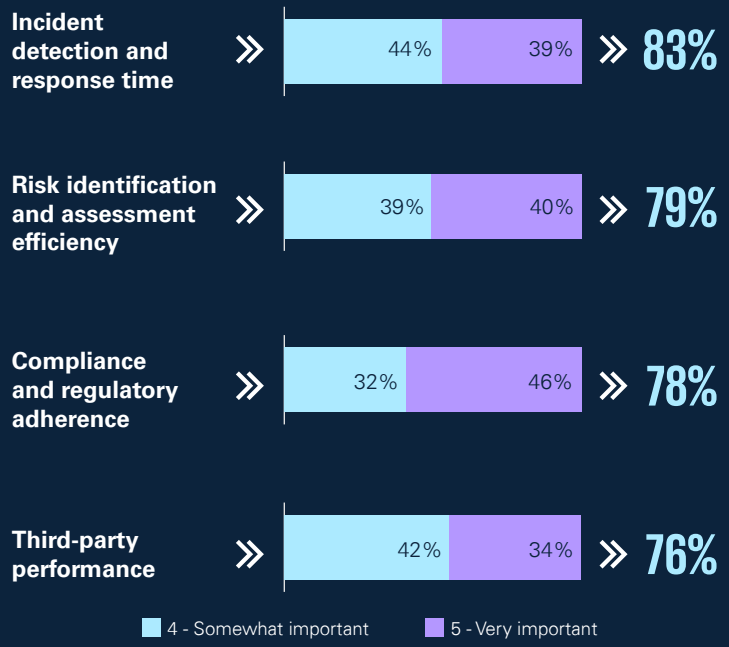
Strategies to align TPRM with operational resilience objectives

Clear role definitions are crucial for integrating third-party risk management into operational resilience, ensuring accountability, and coordinated action. Joint risk assessments and regular cross-departmental meetings enable organizations to break down silos, fostering collaboration among risk, compliance, procurement, and IT teams for unified risk views and effective disruption response.



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

Incident detection and response time, compliance adherence, risk assessment efficiency, and third-party performance are top indicators of successful integration. Prioritizing these metrics helps organizations measure and improve the impact of AI-enabled risk management.



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

Key AI/automation technologies for integrating TPRM with operational resilience

AI-driven monitoring, predictive analytics, and machine learning algorithms are increasingly used to strengthen risk detection and response capabilities. Adoption of these technologies supports faster, more accurate identification of threats and enhances overall resilience.

68% AI-driven monitoring and alerting systems

54% Predictive analytics

39% Machine learning algorithms

Plans to advancing TPRM and operational resilience synergy via AI

Organizations are focused on implementing AI technologies, conducting pilot projects, staff training, and vendor collaboration to enhance synergy between TPRM and operational resilience, driving continuous improvement in managing evolving risks.

56% Implementing new AI technologies

50% Conducting pilot projects or proofs of concept | Training staff on AI and automation

48% Collaborating with vendors on AI/automation solutions

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

For financial services firms, 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, financial services 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 financial services organization but also sharpen its competitive edge in a highly regulated market.

Focus your firepower.

Financial services firms must shift from broad, inefficient screening to a laser-focused, risk-based model. By concentrating resources on the small fraction of vendors that pose a genuine threat to the firm's financial stability and customer data, you'll gain deeper insights where it matters most and stop wasting effort on low-risk relationships. This is especially critical in financial services, where the vendor ecosystem can be vast and complex.

Break down the silos.

True resilience is impossible when risk management is a fractured discipline, a common challenge in large financial services organizations. Integrate your TPRM and ERM functions to create a unified, enterprise-wide view of risk that informs strategic decisions, not just the compliance reports mandated by financial services regulators.

Treat data as a strategic asset.

A financial services TPRM program is only as good as the data that fuels it. Invest in data governance to create a single source of truth, especially when dealing with sensitive customer financial data. Clean, reliable data is the non-negotiable foundation for effective AI, credible reporting for regulators and stakeholders, and confident decision-making in the fast-paced financial services environment.

Move beyond "AI theater."

Don't just claim to use AI—deploy it with purpose. For financial services, this means embedding automation and intelligent workflows across the entire TPRM lifecycle to accelerate processes like KYC/AML checks, uncover hidden risks in the complex web of third-party relationships, and free up your team for more strategic work that enhances the firm's resilience.

Look beyond your own backyard.

In the financial services industry, risk exposure doesn't end with your direct vendors. Develop "Nth-party" visibility to understand the risks lurking deeper in your supply chain, such as dependencies on critical financial market infrastructures or technology providers. This enables you to manage concentration risk and prevent unforeseen disruptions that could impact financial stability.

Outsource outcomes, not ownership.

Financial services firms can leverage managed services to scale capabilities and drive efficiency in high-volume activities like customer onboarding and due diligence. However, the firm must retain firm control over governance and strategy, ensuring that external partners operate as an extension of its risk appetite, not a replacement for it, in line with regulatory expectations for the financial services sector.

Contact us

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

Manish D. Madhavani
Partner,
US Financial Services Leader
KPMG LLP
E: mmadhavani@kpmg.com

Anand Desai
Principal, US Financial Services Leader for Risk Services
KPMG LLP
E: ananddesai@kpmg.com

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

Diana Keele
Managing Director,
Risk Services
KPMG LLP
E: dkeele@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**