KPMG

Global TPRM survey 2026 Report

Healthcare and Life Sciences (HCLS)

The 2025 Global Third-Party Risk Management (TPRM) Survey gathered input from 851 senior leaders across 16 countries worldwide, including 178 participants from the Healthcare and Life Sciences (HCLS) sector. Respondents represent organizations across biotechnology, pharmaceuticals, medical devices, healthcare providers, and related subsectors, offering a comprehensive view of how HCLS teams are approaching third-party risk management amid increasing regulatory and operational complexity.

Organizations are sharpening their focus on regulatory compliance, data governance, and cost efficiency as the primary drivers of third-party risk management. Despite these priorities, they face persistent challenges in monitoring third-party performance, developing contingency plans, and integrating risk management programs. Investment is being directed toward strengthening compliance controls, enhancing risk assessment processes, and adopting technology solutions, reflecting a strategic shift toward more resilient and efficient TPRM practices.

Key drivers of TPRM activity in organizations

Organizations are prioritizing compliance with regulations, data governance, and cost efficiency as the main forces shaping third-party risk management. These drivers reflect a heightened focus on regulatory expectations and the need to safeguard sensitive information while optimizing resources.

51% Ensuring compliance with regulations

34% Data governance and privacy

32% Improving cost efficiency

Top 3 challenges of TPRM

Monitoring performance of third-party and its alignment with procedures	19%
Developing and maintaining exit and contingency plans for critical suppliers	18%
Having enough internal resources	18%
Integrating and aligning with other risk management programs	17%
Determining which third-parties are critical to our organization	17%

The most pressing challenges include monitoring third-party performance, developing contingency plans for critical suppliers, and ensuring sufficient internal resources. Additional hurdles involve integrating risk management programs and identifying which third parties are most critical, underscoring the complexity and scale of today's risk landscape.

Key TPRM spending priorities for the next 12 months

Investment is concentrated on regulatory compliance and audits, risk assessment and due diligence, and technology solutions for TPRM. This spending pattern highlights the emphasis on strengthening controls, improving assessment processes, and leveraging technology to enhance risk management capabilities.

56% Regulatory compliance and audits

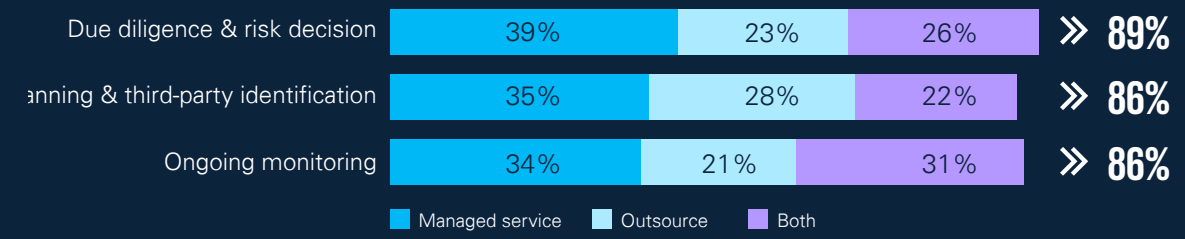
53% Risk assessment and due diligence procedures

41% Technology and tools for TPRM

Managed services and outsourcing are central to streamlining third-party risk management, particularly for due diligence, planning, and monitoring. Organizations prioritize rapid onboarding for critical vendors, while high and moderate risk relationships require more time and scrutiny. The onboarding process is shaped by risk management, security protocols, and access controls, highlighting the balance between speed and thorough risk assessment in building resilient third-party ecosystems.

TPRM areas utilizing managed services and/or outsourcing

Organizations are increasingly leveraging managed services and outsourcing for core TPRM activities, with the highest adoption in due diligence, risk decision-making, planning, and ongoing monitoring. This approach enables greater efficiency and scalability, allowing internal teams to focus on strategic oversight while external partners handle high-volume tasks.



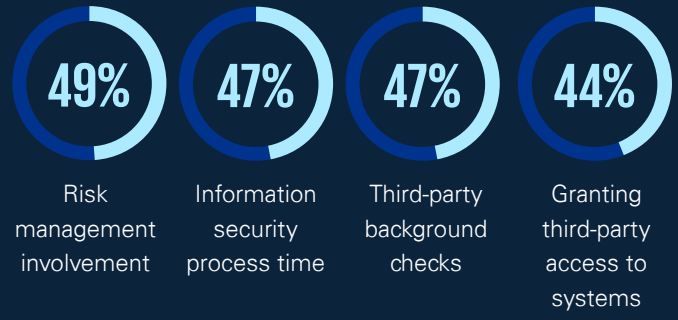
Average time to onboard selected third-party by risk level

Critical third parties are onboarded more quickly, with most completed within 30 days, while high- and moderate- risk vendors tend to have longer onboarding timelines. This reflects a prioritization of speed for the most essential relationships, balancing thoroughness with the need to mitigate urgent risks.

Level of importance	0-30 days	30-60 days
Critical	57%	15%
High	44%	39%
Moderate	37%	44%

Key factors affecting third-party onboarding duration

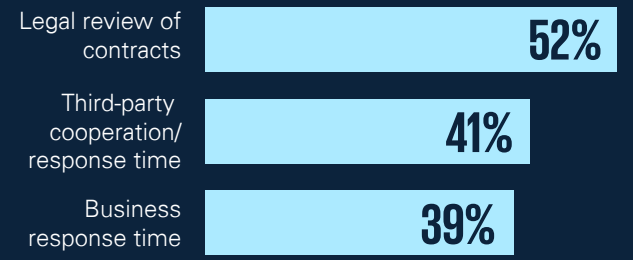
Risk management involvement, information security process time, third-party background checks, and granting access to systems are the main factors influencing onboarding duration. These steps are essential for maintaining robust controls but can extend timelines, especially when multiple teams and systems are involved.



Delays in third-party assessments often stem from legal reviews, partner cooperation, and internal response times. Regulatory compliance, cybersecurity, and legal risks are rising in importance, reflecting a more complex risk environment. Reputational, financial, and supply chain disruptions linked to third parties have occurred repeatedly in recent years, while limited integration between third-party risk management and enterprise risk management continues to challenge efforts to create a unified risk strategy.

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

Legal review of contracts, third-party cooperation, and business response times are the primary factors influencing how quickly third-party assessments progress to contract signing. These steps often introduce delays, reflecting the complexity of aligning legal, operational, and external partner requirements.



Emerging risks gaining importance in TPRM over recent years

Regulatory and compliance risk, cyber risk/information security, and legal risk have become increasingly prominent concerns for organizations. This shift highlights the evolving threat landscape and the need for more robust risk management strategies.

48% Regulatory and compliance risk

35% Cyber risk/ information security

29% Legal risk

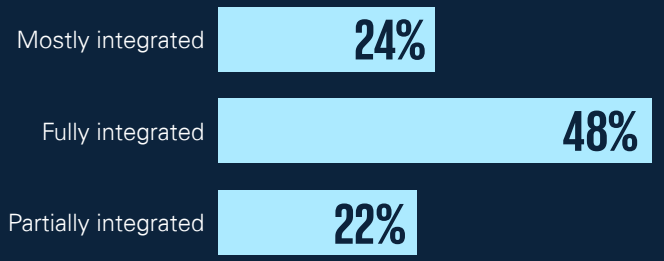
Organizations' experience with third-party issues in the last three years

Significant reputational damage, monetary loss, and supply chain disruption have affected organizations multiple times over the past three years. These recurring issues underscore the tangible impact of third-party risks and the importance of proactive management.

	1-2 times	3-5 times
Significant reputational damage	29%	10%
Significant monetary loss	28%	20%
Significant supply chain disruption	19%	22%

Integration level between TPRM and ERM programs

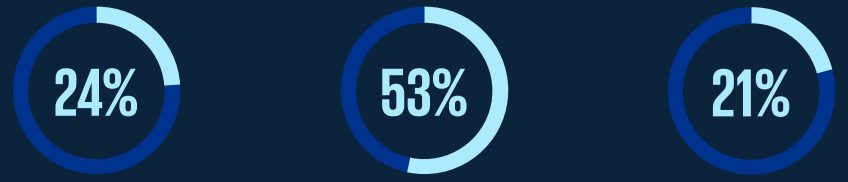
Only a minority of organizations have fully integrated their TPRM and ERM programs, with most reporting partial or moderate integration. This gap points to ongoing challenges in achieving a unified approach to risk management across the enterprise.



A strong focus on integrating third-party and enterprise risk management is driving efforts to create more unified and strategic risk oversight. Proactive incident management, high confidence in data quality, and streamlined technology adoption are shaping the future of TPRM, enabling organizations to respond effectively to disruptions and build resilient risk management programs.

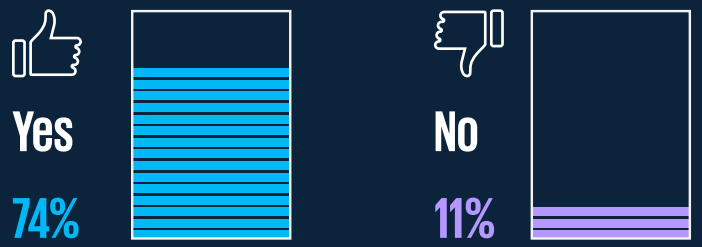
Confidence in data quality and reliability that support TPRM programs

Confidence in the data supporting TPRM programs is generally high, with most respondents expressing either confidence or strong confidence in their data quality and reliability. This foundation is essential for effective risk management and informed decision-making.



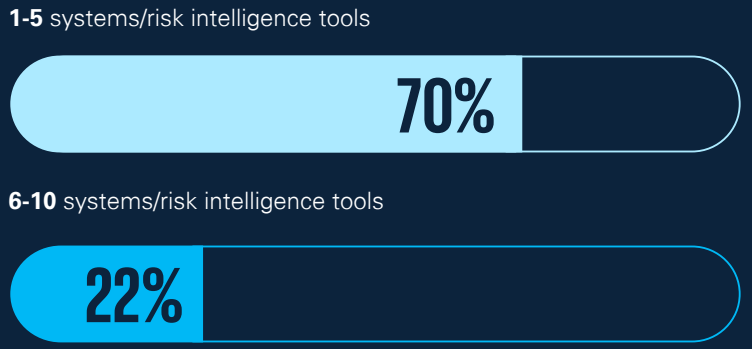
Plans for further TPRM and ERM integration in the next three years

Most respondents intend to deepen integration between third-party and enterprise risk management, aiming for a more cohesive and strategic approach to risk oversight. This reflects a strong commitment to advancing risk management maturity.



Number of systems/risk intelligence tools supporting the TPRM program

The majority of programs are supported by a limited number of systems or risk intelligence tools, with most organizations using between one and five tools. This suggests a preference for streamlined technology stacks, though some leverage a broader array of solutions.



Strategies for managing third-party incidents and disruptions

Organizations rely on post-incident reviews, contingency plans, and immediate third-party liaison to address disruptions. These strategies emphasize proactive planning and rapid response to minimize the impact of third-party issues.

Technology integration and data reliability remain key challenges in TPRM. Automation and AI are improving efficiency and reporting, but most programs still use these tools for specific tasks rather than across the full lifecycle.

Most challenging pain points with existing TPRM technology

Integration with other systems, cost of maintenance and upgrades, and data accuracy/reliability are the top technology challenges. These issues can hinder efficiency and limit the effectiveness of risk management processes.

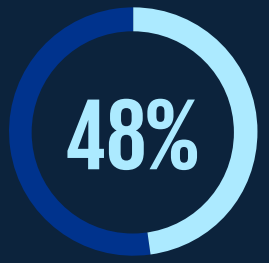
46% Integration with other systems

32% Cost of maintenance and upgrade

31% Data accuracy and reliability

Degree of automation maturity in TPRM

Nearly half of respondents report having moderate automation maturity, characterized by streamlined processes and partial automation within their TPRM programs. This suggestsprogress toward efficiency, though full automation remains a future goal for many.



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% Determine due diligence requirements

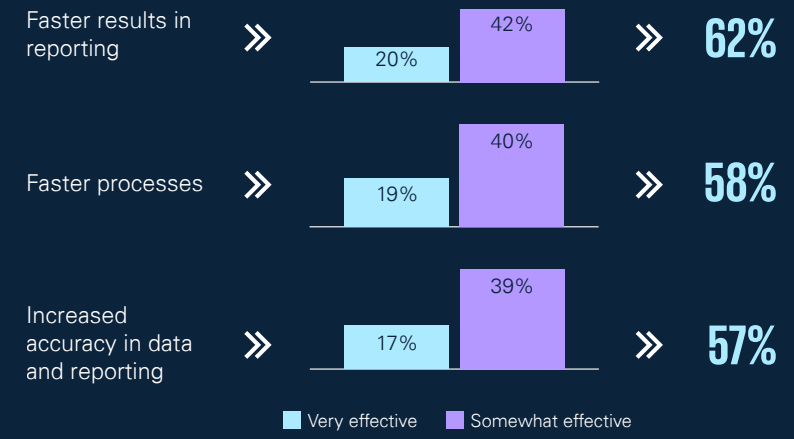
36% Document risk, risk rating, recommendation for an issue

34% Review vendor questionnaire responses and identify issues

Automation is most commonly used for determining due diligence requirements, documenting risk ratings and recommendations, and reviewing vendor questionnaire responses. These targeted deployments help accelerate specific tasks but are not yet applied end-to-end.

Effectiveness of AI in enhancing TPRM processes

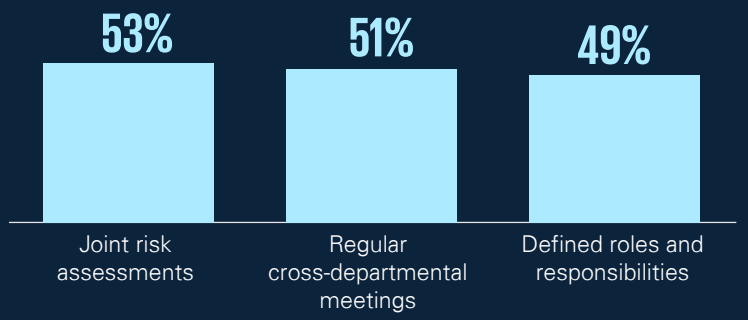
AI is delivering faster results in reporting, speeding up processes, and improving data accuracy, with most respondents finding these enhancements at least somewhat effective. The impact is strongest in reporting, followed by process acceleration and data reliability.



Unified risk assessments, cross-functional collaboration, and clear roles are central to aligning TPRM with operational resilience. Success is measured by compliance, efficient risk identification, and rapid incident response, supported by advanced AI and automation technologies. Organizations are investing in staff training, pilot projects, and technology expansion to strengthen resilience and drive continuous improvement.

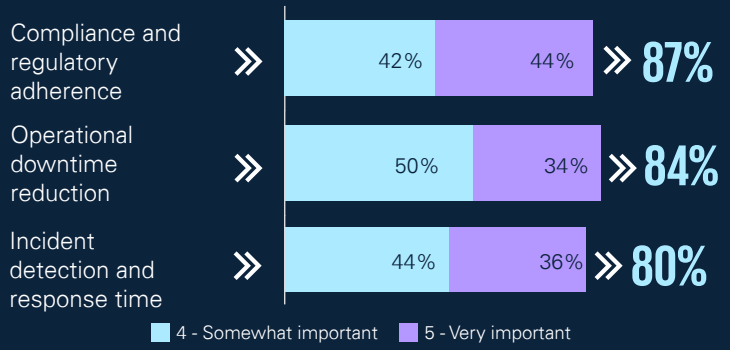
Strategies for ensuring alignment between TPRM and operational resilience objectives

Joint risk assessments, regular cross-departmental meetings, and clearly defined roles are the top strategies for aligning third-party risk management with operational resilience. These approaches foster a unified response to disruptions and strengthen organizational preparedness.



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

Compliance, risk identification efficiency, and incident detection are considered the most important measures of success when integrating AI into TPRM and operational resilience. High importance is placed on regulatory adherence and the ability to quickly identify and respond to risks.



Numbers not to intended to equal 100%. Data displays where respondents selected somewhat important or very important.

Key AI/automation technologies integrating TPRM with operational resilience

57% Predictive analytics

50% AI-driven monitoring and alerting systems

41% Machine learning algorithms

Predictive analytics, AI-driven monitoring and alerting systems, and machine learning algorithms are the leading technologies supporting integration. These tools enable proactive risk management and enhance resilience against disruptions.

Plans for advancing TPRM and operational resilience synergy through AI

Training staff, conducting pilot projects, implementing new AI technologies, and expanding the use of existing solutions to advance synergy between TPRM and operational resilience are focal points for organizations. These efforts aim to build expertise and accelerate adoption of innovative approaches.

48% Training staff on AI and automation

48% Conducting pilot projects or proofs of concept

43% Implementing new AI technologies

42% AI-driven monitoring and alerting systems

Contact us

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