
How can building confidence in AI help navigate your third-party risk transformation?
The better the prompt.
The better the answer.
The better the world works.
EY
Shape the future with confidence

Introduction

The 2025 EY Global Third-Party Risk Management Survey reveals new approaches to managing risks from third parties in a more volatile environment.

It's a crisp autumn day in Frankfurt. The location is the headquarters of a large consumer products company. Maya, a manager in the company's new RiskAI Hub — the AI-powered centralized control tower responsible for coordinating third-party risk management (TPRM) across the global enterprise — receives an alert from Orion, her AI assistant. Orion is picking up a spike in negative social media sentiment related to a critical Tier-2 supplier in Southeast Asia. As it tracks the spike, driven by local news coverage of a chemical spill, Orion's predictive analytics model continuously updates the growing likelihood of a major supply chain disruption. Maya asks Orion to keep monitoring the situation and gather data to identify the root causes of the incident, including any lapses in compliance, performance or oversight. As the situation deteriorates, Orion works directly with Vega, its agentic AI counterpart at the supplier, to draft a remediation plan for human review.

This is the future of TPRM. It's a future in which annual or biennial risk assessments have been replaced by 24/7 real-time monitoring based on sophisticated market sensing using a wide spectrum of data. It's a world in which the use of AI agents enables TPRM to be streamlined and centralized as never before. It's a future that may be a lot closer than many assume — and one that is sorely needed in a transformed external risk environment.

A confluence of trends has shaken up the external risk environment in recent years. Global supply chains have been buffeted by repeated shocks — precipitated by the pandemic, geopolitical conflicts and climate change — drawing greater attention to the resilience of suppliers and potential third-party impacts. The rising number of cyberattacks — the IMF estimates that losses from cyberattacks have more than doubled since the pandemic and more than quadrupled since 2017 — has increased the potential for cyber risk via third-party relationships. Heightened regulatory scrutiny and stakeholder pressures have brought increased focus on third-party practices related to a host of compliance risks, ranging from data privacy to environmental standards.

In brief

- Risk leaders are using AI and centralization to fundamentally transform their third-party risk management functions for the future.
- Operational and cybersecurity risks are growing while the number and complexity of third-party relationships increases.
- Business uncertainty and cost pressures are driving efficiency imperatives for third-party risk management.

> "Approaches are increasingly misaligned with today's competing demands and complex risk environment. TPRM has never been more ripe for transformation.

Amy Gennarini
EY Global Risk Consulting Technology Leader

These developments are emblematic of a new environment in which risks are more interconnected, nonlinear, accelerating and volatile than in the pre-pandemic world.

Unfortunately, today's TPRM is fundamentally misaligned with this new risk environment. Amid accelerating change, TPRM relies on slow and intermittent processes. In a world of interconnected risks, it is siloed and uncoordinated. Against a backdrop of nonlinear growth and unanticipated tipping points that require agility and innovation, it has been slow to adapt. And at a time of tremendous disruption — when companies need to reinvent business models and find new ways of creating value — TPRM is typically disconnected from overall business metrics and strategic objectives.

For many years, the move to centralize TPRM programs has provided a path to address at least some of these sources of misalignment. Yet, while the adoption of centralized approaches has grown over time, organizational constraints often hinder more extensive implementation, and it is only by addressing these that companies will realize its full potential. Artificial intelligence (AI) provides a way to accelerate the centralization journey.

But the bigger opportunity with AI is in using it to fundamentally reinvent TPRM, making it more resilient and aligned with the new risk environment. In a faster-paced, more volatile world, AI can conduct real-time risk monitoring at massive scale by analyzing continuous data feeds such as news alerts, financial data, and social media streams and synthesizing these external inputs with the company's internal operating data. In an environment of interconnected risks and nonlinear change, AI can be used to simulate scenarios and impacts, helping overcome human failures of imagination.

"Many companies have repeatedly focused on solving the last problem — the COVID-19 pandemic, supply chain resilience, and so on — rather than approaching TPRM strategically and cohesively," says Amy Gennarini, EY Global Risk Consulting Technology Leader. "While regulations in sectors such as financial services have pushed those firms to look at risk holistically, many others still address it in pockets or siloes. Such approaches are increasingly misaligned with today's competing demands and complex risk environment. TPRM has never been more ripe for transformation."

The 2025 edition of the EY Global Third-Party Risk Management Survey has valuable insights for leaders navigating this challenging space. Conducted in collaboration with Oxford Economics, the survey seeks to understand how organizations handle TPRM, including best practices, challenges and outlook.

About the 2025 EY Global Third-Party Risk Management Survey

The survey includes 500 executives that lead or assist TPRM. Surveyed organizations have revenues of $250 million or more, and 20% are listed on the Fortune 500. Responding companies are headquartered in the US, Canada, UK, France, Germany, Spain, Italy, Nordics, India, China, Singapore, Japan, or Australia, and come from a broad spectrum of industries: Banking and Capital Markets, Insurance (Financial Services/Non-Health Care), Other Financial Services (e.g., Fintech), Private Equity, Wealth and Asset Management, Advanced Manufacturing and Mobility, Technology, Media and Entertainment, Power and Utilities, Health care (including health care insurance, providers, payers, etc.), Life Sciences, Consumer and Retail, Professional Services, Government Agency, and Oil and Gas.

More complex relationships with more third parties create new challenges

Our survey reveals changing risk priorities for leaders as the risk environment becomes more volatile and business challenges increase pressure on efficiency.

The new risk environment is striking at a time when risk managers already face growing business pressures within their organizations. "The number of third-party relationships managed by a typical company has risen sharply in recent years, as has the complexity of these relationships," says Kapish Vanvaria, EY Global Risk Consulting Leader. "Meanwhile, an environment of lingering business uncertainty and cost pressures is creating an imperative for leaders to conduct third-party risk management in a more effective way. AI has proven to be a game changer in this arena."

Companies are dealing with multiple third-party risks — and taking a tougher line

The competing challenges posed by the new risk environment are visible in the survey responses. These include an increased emphasis on operational resilience and cybersecurity.

> "An environment of lingering business uncertainty and cost pressures is creating an imperative for leaders to conduct third-party risk management in a more effective way. AI has proven to be a game changer.
>
> **Kapish Vanvaria**
> EY Global Risk Consulting Leader

"Operational risk" has jumped to the top spot among factors companies consider when monitoring subcontractors, replacing "concentration risk" in the 2023 survey. In the current survey, 57% of respondents cite operational risk as a factor they consider, a significant increase from 40% in the 2023 survey. A similar shift is visible in the criteria used to identify critical third parties — entities whose disruption or failure could significantly impact the organization's ability to operate. While "financial impact" remains the most important criterion used to define a critical third party (43%), this is closely followed by "criticality of the business process/function," at 39%. Meanwhile, "business continuity and resilience" has recorded the steepest increase in importance, jumping from 14% in 2023 to 23% in the current survey.

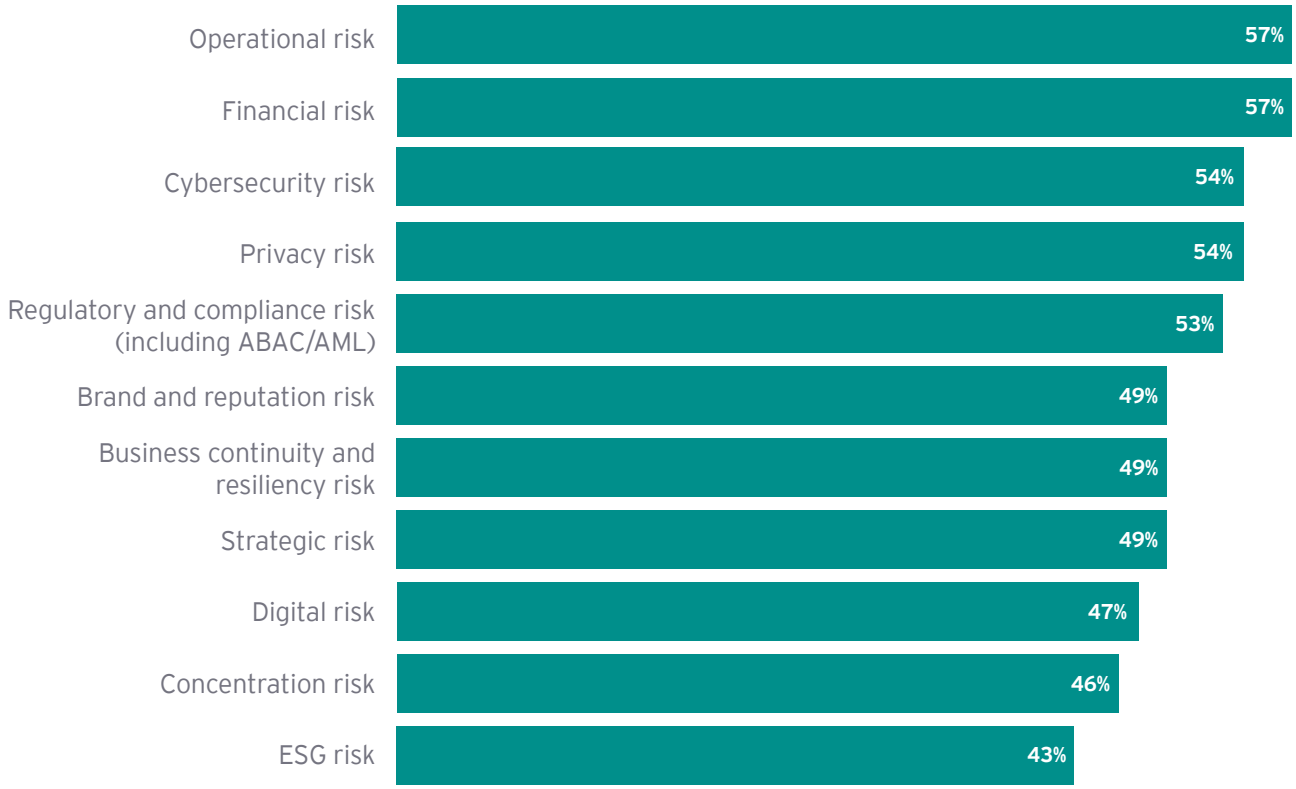
Operational risk

57%

of respondents cite operational risk as a consideration for third parties, compared to 40% in 2023.

Operational risk rises as the top consideration

To what extent does your organization consider the following risks when monitoring third parties?



Note: Percentages do not add up to 100% due to the respondent's ability to choose multiple responses.

One way in which companies are responding to these heightened risks is by cracking down during control assessments of third parties. If third parties don't respond to questionnaires in a timely manner, companies are now more likely to escalate enterprise processes (87% of respondents, up from 70% in 2023) or even cease operations entirely (29% vs 17% in 2023). When risks are identified during assessments, companies are far more inclined than before to take the path of remediation, with 57% of respondents saying they choose remediation, compared to only 17% in 2023.

The number and complexity of third-party relationships is increasing

While companies have always dealt with third parties, the number and complexity of such relationships has grown in recent years. A challenging business climate has driven an imperative to do more with less, and companies have often turned to third parties to unlock operating efficiencies. The adoption of digital transformation initiatives has expanded the third-party ecosystem, with companies increasingly using third parties for cloud services, software-as-a-service (SaaS) providers, and other digital platforms.

The end result is that companies rely more than ever on large numbers of specialized service providers. Today's financial services companies, for instance, partner with a host of fintech service providers, including payment processors, loan providers and investment platforms. Healthcare companies rely on third-party vendors for services such as telemedicine, electronic health records and medical supplies. Across sectors, companies are turning to third-party service providers for everything from human resources to business intelligence and supply chain logistics.

The end result is that companies rely more than ever on large numbers of specialized service providers. Today's financial services companies, for instance, partner with a host of fintech service providers, including payment processors, loan providers and investment platforms. Healthcare companies rely on third-party vendors for services such as telemedicine, electronic health records and medical supplies. Across sectors, companies are turning to third-party service providers for everything from human resources to business intelligence and supply chain logistics.

This, in turn, has increased the number of business functions that rely on third parties and are exposed to third-party risks. In the past, a bank may have had one or two risk verticals that cared about third-party risk; today, that number could be in excess of 20.

The ascendance of these specialized service providers hasn't just increased the number of third-party relationships; it has also increased their complexity. In the past, many of these activities might have been performed manually within the safety of a company's environment, or at most with an application programming interface (API) that connected to the company's environment. Today, those same activities may involve a network of third parties working in environments that are not owned or controlled by the company. In turn, those third parties engage with their own networks of third parties to deliver services. The bottom line is that "third-party risk management" is already something of a misnomer — today's companies have to cast a wider net to consider not just third-party risks, but also fourth-party, fifth-party and nth-party risks.

The complexity of the third-party ecosystem is further complicated by the increased reliance on non-traditional third parties (NTTPs), such as strategic partnerships, resellers, broker-dealers, legal third parties, and others.

The survey results reflect these trends. Navigating the risks related to an increasing number of third parties continues to be a vital function for TPRM programs. The challenge is particularly acute for newer, less mature TPRM programs, which actively manage more third parties than do established programs (which actively manage fewer third parties by adopting risk-based prioritization). TPRM programs that are less than three years old manage a median of 275 third parties, while those that have been around for over a decade manage a median of 80 third parties. Survey respondents report an increasing burden related to monitoring NTTPs. Across all types, the number of NTTPs monitored increased by an average of 20% relative to last year. Companies are also expending resources monitoring nth party risks, with almost two-thirds (64%) of respondents saying that "third-party diligence includes validation of their TPRM program as well as the risk/control assessment of their third-party population and their subcontractors."

The number of business functions relying on third parties and that are exposed to third-party risks has greatly increased. In the past, a bank may have had one or two risk verticals that cared about third-party risk; today, that number could be in excess of 20.

AI creates an unprecedented opportunity to reinvent TPRM

AI and increased centralization are helping companies navigate complicated paths in TPRM like never before.

TPRM functions need new ways of operating to address the competing pressures of the new risk environment, the increasing number and complexity of third-party relationships, and the need to do more with less. TPRM transformation is a journey, from seeking marginal efficiency gains at the near end, to fundamental transformation at the other. Companies have been on this journey for a while, most notably with the drive toward increased centralization. The emergence of AI provides an opportunity to both accelerate centralization and transform TPRM.

TPRM centralization has started companies on the path to greater efficiency

Continuing a multi-year pattern, the 2025 survey shows a trend toward increased centralization of TPRM. A growing number of organizations use centralized, enterprise-wide TPRM programs (57% in 2025, up from 54% in 2023).

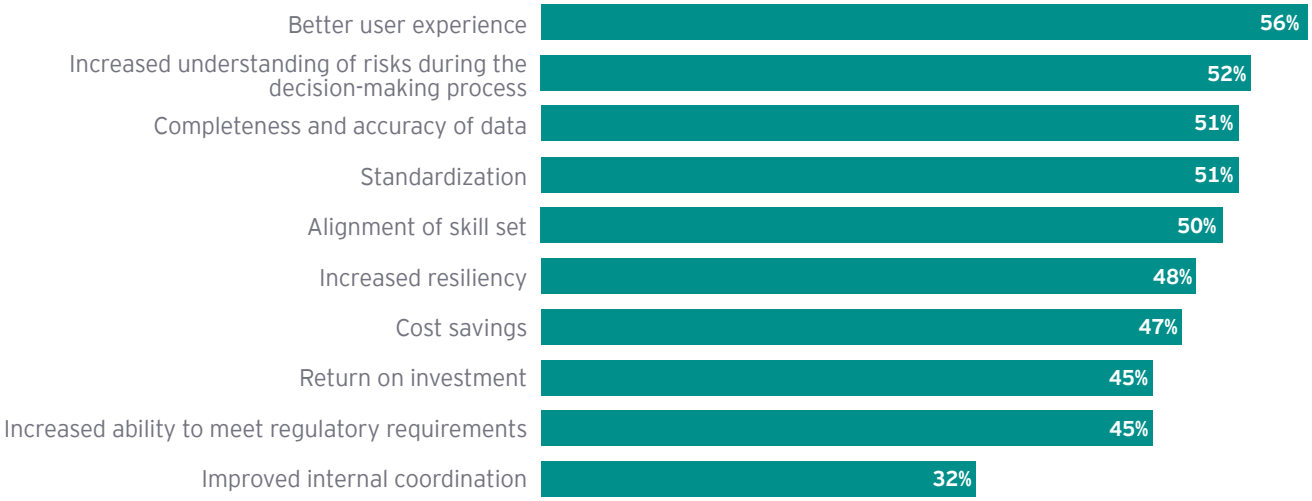
TPRM centralization offers many benefits. It reduces friction points; instead of reaching out to the same third party multiple times, often with duplicative and partially redundant requests, outreach can be done once and in a coordinated, streamlined way. The survey data suggest that many organizations could benefit from such streamlining. When performing control assessments, about four in ten companies (43%) still use multiple questionnaires for different risk domains. They send third parties an average of 55 questionnaires. Add to this the compliance burden of each additional questionnaire (45% of respondents say that control assessment questionnaires have 101 to 200 questions, while another 36% have between 201 and 350 questions) and it's apparent there's much room for a centralized approach to reduce the compliance burden and friction points with third parties.

Critically, centralized TPRM allows for better coordination and more holistic risk assessment. "A centralized approach to TPRM allows an organization to connect dots across verticals and see the big picture," says Rohit Mathur, EY Global Risk Consulting Strategy Leader and EMEIA Risk Consulting Leader, "For instance, an organization's Cybersecurity team may be monitoring a third party with respect to cyber risk. That third party might have robust cyber controls and score highly with respect to cyber risk. But the party may simultaneously be hemorrhaging money, with a high likelihood of bankruptcy in the next six months — which would obviously jeopardize its ability to invest in cyber controls going forward. If the organization does not connect dots across cyber and financial risk, it would miss the overall picture."

The benefits of centralization are visible in the survey data. Ninety-two percent of organizations with a centralized TPRM structure have directly invested in improving and optimizing the program's capabilities and effectiveness. The key benefits reported from this maturation include a better user experience (56%), increased understanding of risks during the decision-making process (52%), completeness and accuracy of data (51%) and standardization (51%).

User experience and increased understanding of risks continue to be the top benefits

What benefits has centralization brought to your TPRM program?



Note: Percentages do not add up to 100% due to the respondent's ability to choose multiple responses.

Centralized TPRM structures also show greater maturity several key areas when compared to hybrid structures. They are more mature in third-party inventory (58% centralized vs. 39% hybrid), risk models (51% centralized vs. 36% hybrid), assessment methodology (49% centralized vs. 33% hybrid), policies and standards (46% centralized vs. 31% hybrid), and governance and oversight (43% centralized vs. 29% hybrid).

AI is a value catalyst and opportunity to reinvent TPRM

AI has tremendous potential to disrupt TPRM, enabling not just greater efficiencies but also a fundamentally different approach to identifying, monitoring and managing third-party risks.

The early use cases adopted by companies will often focus on using AI to automate existing manual processes and generate operating efficiencies. This includes streamlining repetitive tasks — such as data collection, initial risk assessments and vendor onboarding — and speeding up risk assessments. Beyond this, the true potential of AI is not in automating existing processes as much as in deploying it to create value by conducting TPRM in fundamentally different ways.

Consider how AI could create significant efficiencies and reinvent traditional ways of working, across different stages of the TPRM life cycle:

- **Vendor identification:** Instead of manually compiling vendor lists, AI uses algorithms to scan databases and identify vendors based on predefined criteria, making the process faster and more comprehensive.
- **Risk assessment:** AI models assess risks based on historical data and predictive analytics, providing objective risk scores.
- **Due diligence:** AI replaces slow and labor-intensive manual document reviews with automated collection and analysis of vendor documentation, such as financials and compliance records.
- **Contract negotiation:** AI analyzes contract terms using natural language processing (NLP) to identify risks and suggest improvements based on best practices.
- **Onboarding:** AI streamlines the onboarding process through automated workflows and checklists, while solidifying compliance with requirements.
- **Monitoring:** AI continuously monitors vendor performance using real-time data analytics and alerts for any anomalies or compliance issues.
- **Incident management:** AI utilizes predictive analytics to identify potential incidents before they occur and conducts scenario analysis to foresee "domino-effect" risks that may be hidden in more linear and siloed approaches.
- **Training and awareness:** AI provides personalized training modules based on individual employee needs and learning styles.

Despite its potential, AI adoption in TPRM is still relatively low. Only 13% of companies have optimized technology and automation within their TPRM programs (or achieved "Level 5" maturity).

"AI usage is in its infancy," says Gennarini. "So far, most TPRM functions are only deploying AI at low scale and are using capabilities that have been around a long time, such as optical character recognition (OCR) in document search."

The new generation of AI models, including agentic AI, will move from seeking incremental operating efficiencies to conducting TPRM in fundamentally different ways. For instance, instead of just using OCR and NLP to review contractual terms, a world of AI agents could enable agents to work directly with agents at third parties to negotiate contracts based on market data, business objectives and governance/regulatory requirements. After human review, finalized agreements could be encoded as smart contracts on the blockchain, ensuring transparency and security, as well as automated monitoring of compliance and execution of milestone payments.

The good news is that TPRM functions have the desire to invest in AI and data analytics. The top driver of future investment in TPRM programs is "AI/ML capabilities for enhanced due diligence and contract performance/monitoring" (31% of respondents), while "Data-driven approach to monitor third parties" is second (28%) and "Automation of due diligence for efficiency and heightened risk management purposes" is third (27%).

AI and centralization can catalyze each other

A number of factors hinder more extensive adoption of AI and centralization in TPRM.

Fragmented organizational structures and misaligned incentives lead to a disjointed approach and impede achieving the full value potential of centralization. TPRM is typically not led by a C-level officer; instead, it is a few levels down from C-suite. It is often dispersed across business unit leaders, who only have the remit, incentives and budget to address it within their vertical — rather than to align with other business units and approach it holistically across the enterprise.

While the factors responsible for low AI adoption vary from company to company, common challenges include cost considerations, lack of expertise and data readiness. Furthermore, the breadth and complexity of TPRM makes integrating AI solutions into existing TPRM processes and workflows a difficult undertaking.

The symbiotic relationship between centralization and AI can help overcome some of these barriers and accelerate adoption. For instance, a key pillar of centralized TPRM is harmonizing and centralizing data across the verticals of the organization — but this is also a key prerequisite for AI, so it could help overcome the barrier of data readiness and accelerate AI adoption. By the same token, AI can catalyze centralization, by providing TPRM managers the capabilities to monitor real-time data across the enterprise and third-party ecosystem.

3

Three actions for risk leaders

Leaders can take specific steps now to accelerate transformation and ready their organizations for the changes ahead.

Business and risk leaders can these three actions to accelerate the transformation of TPRM and achieve the full value potential of centralization and AI adoption:

1 Focus on the enterprise

TPRM is conducted in different verticals of the enterprise, which are structured and incentivized to focus on different metrics. Procurement may track contract compliance and vendor performance. Cybersecurity may be focused on incident response time and cost of breaches. Supply chain may care about supplier compliance and resilience metrics.

Yet, realizing the full potential of AI and centralization requires understanding your obligations at an enterprise level — such as regulations, board imperatives, or investor imperatives — as well as how these translate to third-party risks and connect to the metrics of individual business units. If you are only looking at specific risks, instead of how your ecosystem of third parties could impact the overall business, you are narrowing your view and may set yourself up for suboptimal decision making.

We've written previously about the concept of a "risk steward" — someone who is charged with prioritizing risk management requirements across your organizational siloes and driving a connected, proactive risk management approach. TPRM is a true horizontal that cuts across the enterprise, with every internal function having a mirror third-party impact. It would benefit tremendously from a risk steward approach.

2 Invest in AI readiness

The survey responses show that AI adoption in TPRM is low, but that organizations have the ambition to scale up adoption in the years ahead. Bridging that gap and achieving that ambition requires investing in AI readiness.

This includes a thorough assessment of existing TPRM processes, tools, and data management practices to identify gaps and areas for improvement in preparation for AI integration. It includes investing in data readiness to improve data quality, standardizing data formats and implementing data governance. It includes preparing the workforce, by closing skills gaps and investing in training and upskilling.

Critically, it includes monitoring trends, both to keep pace with emerging best practices in TPRM, as well as to prepare for the next waves of AI.

3 Question assumptions and accelerate tipping points

"A decade ago, most companies had policies prohibiting their data from ever touching the public cloud, because of the fear factor of the technology," says Kawther Haciane, EY MENA Digital Risk Leader. "Today, the script has flipped. Companies everywhere are 'cloud first' — everything has migrated to the cloud, and exceptions have to justify why they shouldn't be on the cloud. What happened? We reached a tipping point, the assumptions and economics flipped, and it triggered mass adoption."

Indeed, technology is replete with examples of such tipping points — while the new risk environment is accelerating the pace of nonlinear change, making tipping points increasingly likely. Consider how the launch of ChatGPT upended assumptions about the capabilities of GenAI, and the time frames in which they could be achieved. Or consider something closer to home for TPRM functions: how the COVID-19 pandemic transformed some components of TPRM almost overnight, as the shift to remote work removed the ability to do onsite audits, forcing organizations to embrace technology at scale.

We may now be approaching a similar tipping point for AI adoption in TPRM. As the number and complexity of third-party relationships has swelled in recent years, so too has the friction, pain and cost of doing third-party risk assessments manually. But this is also changing the economics of AI adoption. Once you are doing assessments at larger scale — in the thousands instead of hundreds — you have an increased financial incentive to invest in AI, as well as the expanded scale with which to recoup those investments.

An even bigger tipping point may be imminent in the advancement of the technology. The new generation of AI models — including agentic AI, multimodal AI, reasoning AI, and self-improving AI — are bringing breakthrough capabilities, and combining them could be a game changer for TPRM. This could challenge cost-benefit calculations and make the value proposition of AI irresistible.

The tipping points discussed above have one thing in common: they took most companies by surprise, requiring them to scramble and put together an often-hurried response. But there is another path. By anticipating a tipping point, you can prepare your organization for it. Even better, you can accelerate the shift by taking the steps identified above, to invest in the future, fix misaligned incentives, and realign organizational structures.

TPRM exists to ensure that the rest of the organization isn't caught unawares by external disruptions. Now, more than ever, it may need to apply that focus to itself.

Summary

The 2025 EY Third-Party Risk Management Survey explores how risk leaders are using AI and centralization to transform their TPRM functions for a rapidly evolving risk landscape. They are also making their TPRM functions more efficient and effective to meet heightened business expectations.

Authors

Chris Watson
Global Third-Party Risk Management Leader
christopher.watson@ey.com

Scott McCowan
EY Global Consulting Risk Markets Leader
scott.mccowan@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.