MITRATECH

Rebalancing the Risk Ecosystem:

The Mitratech 2025 Third-Party Risk Management (TPRM) Study

EMPOWER. AUTOMATE. ELEVATE.

Table of Contents:

Executive Summary:

An Ecosystem in Flux: Mounting Pressures, Limited Resources

The 2025 Mitratech Third-Party Risk Management (TPRM) Study paints a vivid picture of an ecosystem under strain. Organizations today are not isolated entities; they are part of expansive, interdependent networks composed of third parties such as vendors, suppliers, and contractors. This intricate ecosystem is being reshaped by shifting regulatory climates, growing operational complexity, and the emergence of new technological species like Artificial Intelligence (AI).

But while the canopy is expanding, the roots remain undernourished. Nearly **70% of TPRM programs continue to be understaffed, managing just 40% of their vendor base on average**. This imbalance leaves the ecosystem vulnerable, with key areas lacking the biodiversity needed for resilience. Regulatory scrutiny is putting pressure on the TPRM ecosystem, driving compliance involvement to an all-time high. Meanwhile, reliance on manual tools continues to undermine risk visibility and incident readiness, even as AI adoption begins to gain cautious momentum.

The ecosystem is aware of the threats in its midst, but it is still evolving to meet them. **Explore the full report** for insights into how leading organizations are addressing these challenges and building more connected, resilient, and forward-looking TPRM programs.

Respondent Profile and Methodology:

Study Overview

In the early Spring of 2025, Mitratech conducted a study on current trends, challenges, and initiatives impacting third-party risk management (TPRM) practitioners worldwide.

The goal of the study — and analysis of its results — is to provide a state-of-the-market overview of third-party risk and deliver actionable recommendations for organizations seeking to grow and mature their third-party risk management (TPRM) programs, specifically related to:

1. Improving manual processes, tools, and coverage of the third-party lifecycle
2. Adopting new technologies, such as AI, to simplify TPRM

Respondent Profile

Respondents held direct responsibilities in third-party risk management, IT vendor risk management, or supplier risk management at companies of all industries and sizes, spanning multiple geographies and overseeing between 40 and 40,000 third-party relationships.

Company Size

The study includes data from organizations of all sizes, ranging from small enterprises with fewer than 100 employees to large corporations with tens of thousands of employees. The diversity in company size offers a broad perspective on the varying TPRM challenges and solutions across different business structures.

Industries

The respondents came from a wide range of industries, including healthcare, financial services, technology, manufacturing, business services, education, biotechnology, retail, energy, entertainment, transportation, construction, government, real estate, insurance, hospitality, and agriculture.

Methodology

The study was conducted through an anonymous survey distributed to TPRM professionals across different sectors. Responses were collected via secure data collection tools, and no confidential information was used in preparing this report.

FINDING 1

The Resource-Starved Habitats: Understaffed and Underprepared

Two-thirds of TPRM programs are understaffed. Programs lack the resources and coordination to adequately manage large vendor ecosystems, assessing only 40% of vendors on average.

In any natural ecosystem, undernourishment can quickly lead to imbalance. The most pressing challenge identified in this year's survey is the acute lack of resources. Conducting vendor risk assessments remains a significant hurdle for largely understaffed and under-resourced teams.

As a result, organizations are only managing, on average, 40% of their vendors. Over two-thirds of respondents claim their TPRM programs are understaffed. In most cases, those teams are understaffed by nearly 30%. In fact, the number one barrier to TPRM program growth or adoption, cited by a staggering 56% of organizations, is a lack of resources.

How many people in your organization are currently involved in assessing third-party vendors/suppliers?

Do you ideally need to assess third-party vendors/suppliers?

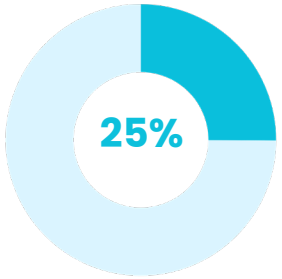
Actual Team Size vs. Ideal Team Size

- 31.5% Actual = Ideal
- 68.5% Actual ≠ Ideal

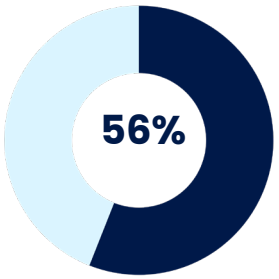
Teams Understaffed By

↓ 29%

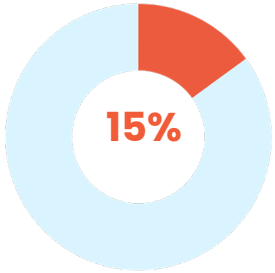
What is the level of program coordination across your organization for the third-party risk management/IT vendor risk management/supplier risk management program?



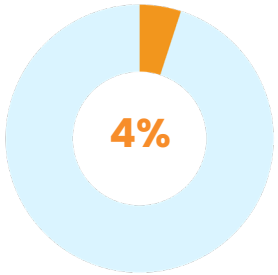
Highly coordinated across the organization



Some coordination across the organization



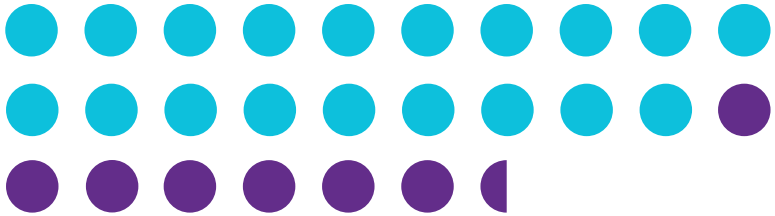
Minimal coordination across the organization



No coordination across the organization

Approximately how many third-party vendors/suppliers does your company work with in total?

Are they actively being managed by your risk program?

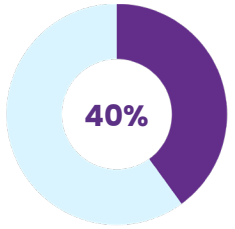


Total Vendors

Vendors Managed

Each Circle = 100 Vendors

Vendors Managed



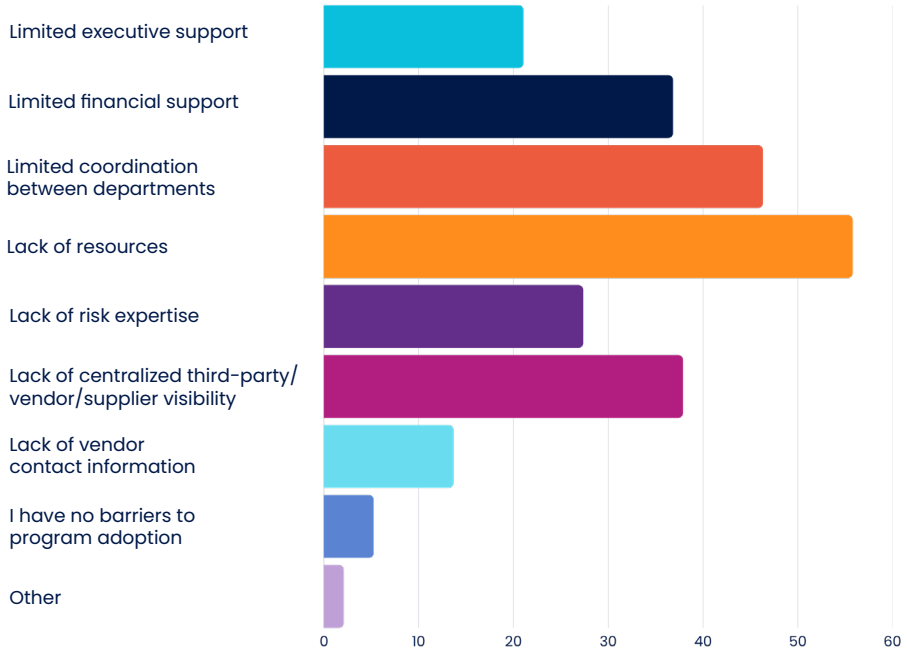
Coordination issues exacerbate this problem: fewer than 1 in 4 programs describe themselves as “highly coordinated,” and over 45% cite departmental silos as a key barrier to growth and maturity.

This lack of coordination hinders visibility, with the third-highest barrier to program adoption being a lack of centralized visibility for third-party vendors and suppliers (38%).

In many cases, those in charge of managing vendor relationships are not the same as those in charge of managing vendor risk.

Year over year, infosec and risk management teams continue to own the overall program, while business owners manage the relationships and procurement oversees the vendor or supplier database. Companies recognize the importance of collaboration but continue to struggle with operationalizing connected efforts. There may be a glimmer of hope, though, as organizations start to distribute ownership of vendor data more evenly.

What are the top barriers to adopting or growing your third-party risk management program?



FINDING 2

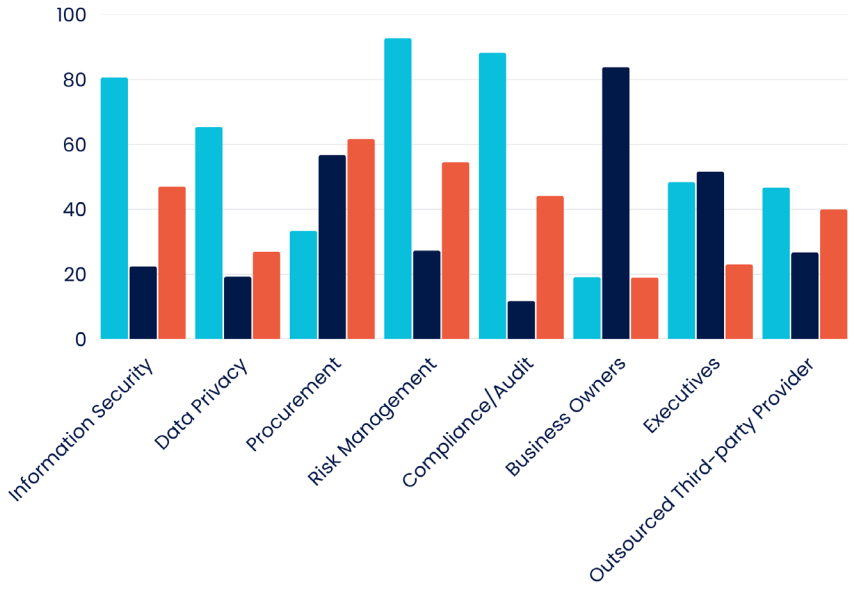
Regulatory Climate Change Reshapes the Risk Ecosystem

The involvement of the compliance team in TPRM has surged from 42% in 2023 to 88% in 2025, as increasing regulatory scrutiny drives deeper third-party oversight and cross-functional accountability.

In every ecosystem, climate is a defining force. It shapes the terrain, influences migration patterns, and determines which species adapt and which fall behind. In the third-party risk ecosystem, regulation is the climate, and in 2025, the temperature has spiked.

Regulatory scrutiny — particularly around data privacy and operational resilience — has intensified like a fast-changing climate, accelerating the involvement of compliance teams in TPRM. The presence of compliance teams soared to 88% in 2025, up from just 42% in 2023. Over half of organizations say regulatory oversight has directly increased the scrutiny they apply to third parties. This pressure is driving efforts to improve visibility, ownership, and risk coverage across departments.

In your organization, which department:

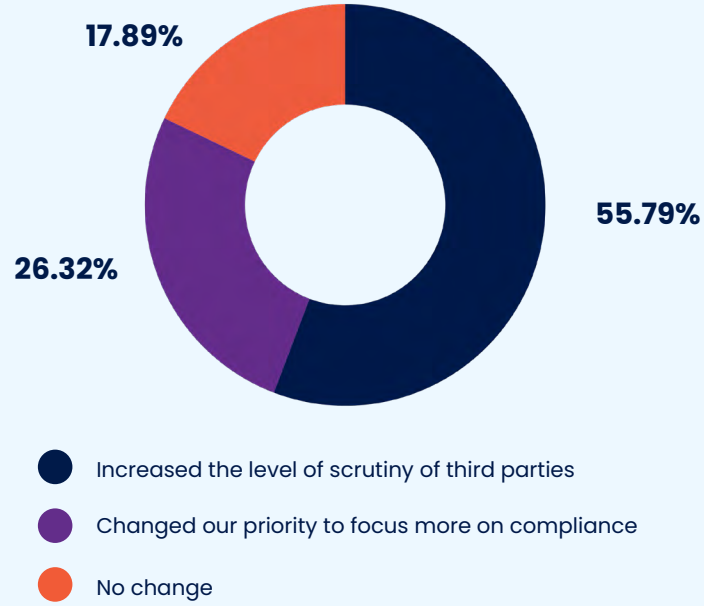


What stands out in this year's survey is the significant increase in ownership and involvement of compliance teams. Compliance / Audit teams show a rise in involvement in 2025 (88.24%) compared to 2024 (68.57%) and 2023 (41.79%). Additionally, increased regulatory scrutiny is the primary reason for changes in program involvement, leading at 54% in this year's study.

Meanwhile, when asked how legislation and/or regulatory oversight has impacted the way organizations monitor third-party risk, the majority of respondents indicate an increase in their scrutiny of third parties, and over a quarter of respondents report shifting priorities to focus more on compliance.

While roles and responsibilities across Infosec & Risk, Business Owners, and Procurement remain consistent with previous findings, the gap in database management vs. program ownership appears to be closing this year with a slight uptick (approximately +10%) in the Risk Management team's role in the operational aspects of managing vendors compared to 2024's survey.

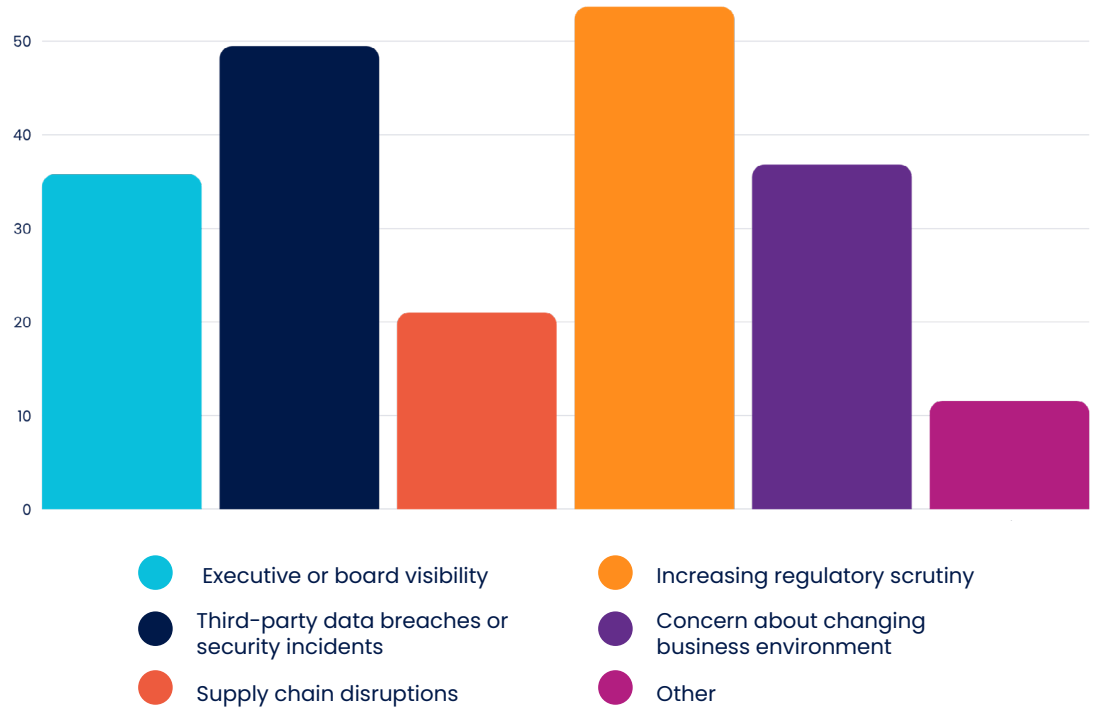
How has legislation and/or regulatory oversight impacted the way your organization monitors third-party risk?



Why does this matter? Departments that once worked in silos are now being pushed to share data and collaborate, much like different species seeking new symbiotic relationships in a changing biome. When data and responsibility are dispersed more evenly across the environment, it fosters ecosystem-wide resilience.

As mentioned in **Finding 1**, lack of coordination and centralized data management are key barriers to TPRM programs. This increased distribution of database ownership may indicate organizational efforts to address visibility issues and reduce the frustrations associated with siloed vendor information.

In general, why has involvement in third-party risk management changed in the last year?



FINDING 3

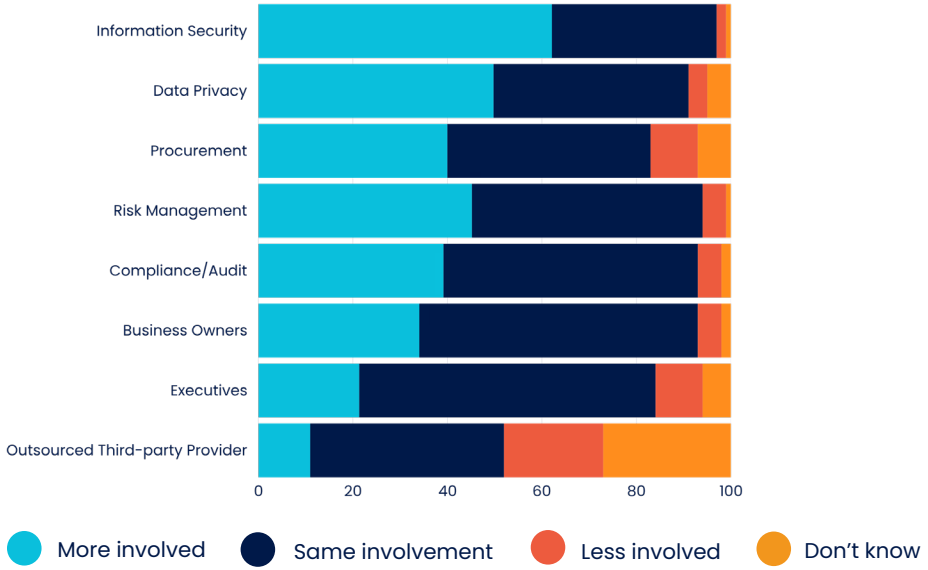
Cybersecurity Remains Paramount, But Diversified Risk Tracking Emerges

Cybersecurity still leads third-party risk oversight at 85%, but teams are swiftly broadening to encompass privacy, compliance, and business continuity threats for a truly holistic risk posture.

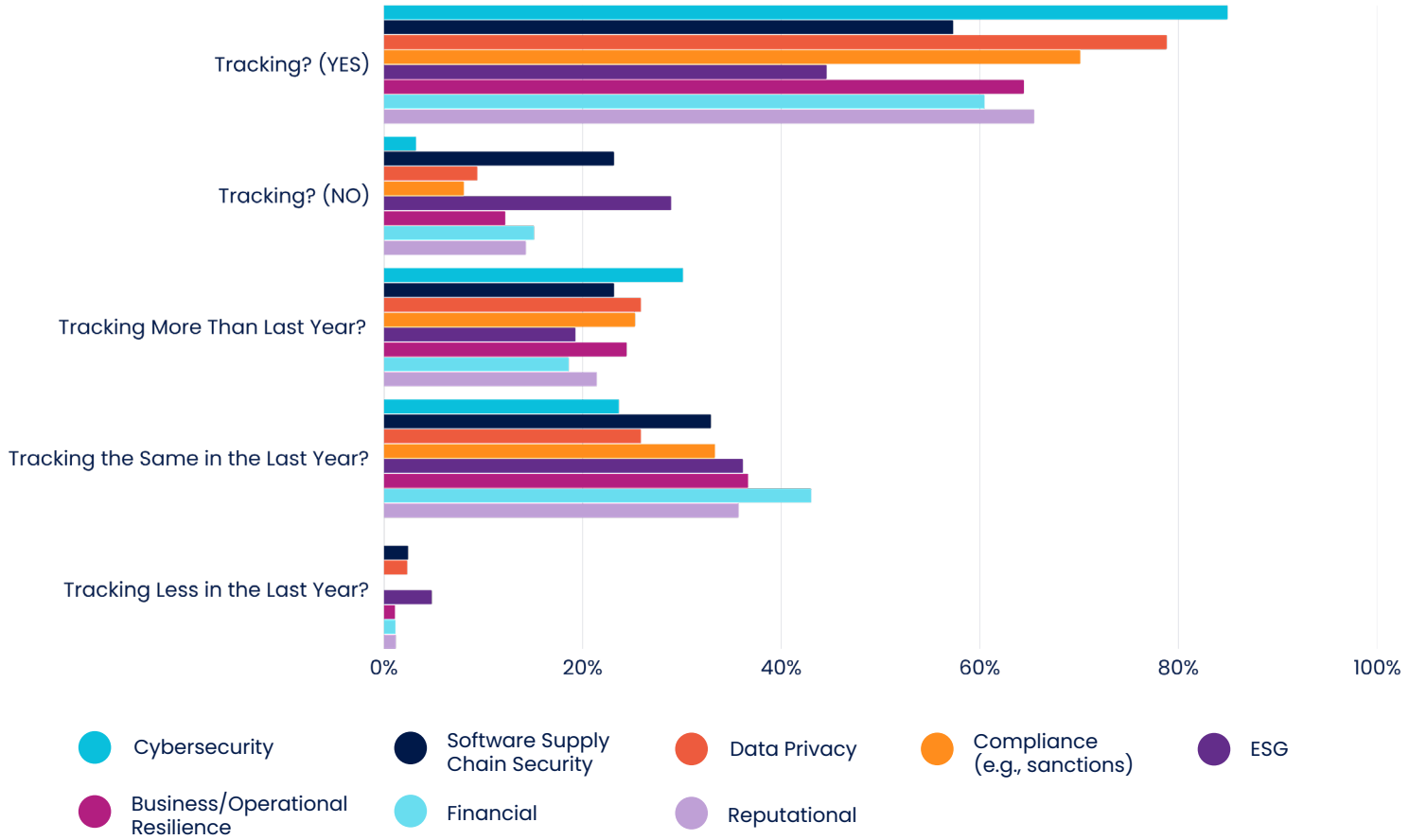
Cybersecurity remains the most tracked third-party risk (85%), with no organizations reporting a decrease in efforts. However, teams are expanding their focus to include Data Privacy (79%), Compliance (70%), and Business Continuity (64%). This diversification reflects the increasingly interconnected nature of third-party risks.

Respondents report that Information Security (62%), Data Privacy (50%), and Risk Management (45%) teams are more involved in third-party risk this year. This finding is consistent with those from the previous year, indicating a continued focus on cybersecurity risk as a strong driver for third-party risk management programs.

In the last year, would you say that these departments are more or less involved in third-party risk management versus the previous year?



What types of third-party risks does your organization track, and how has this changed in the last year?



FINDING 4

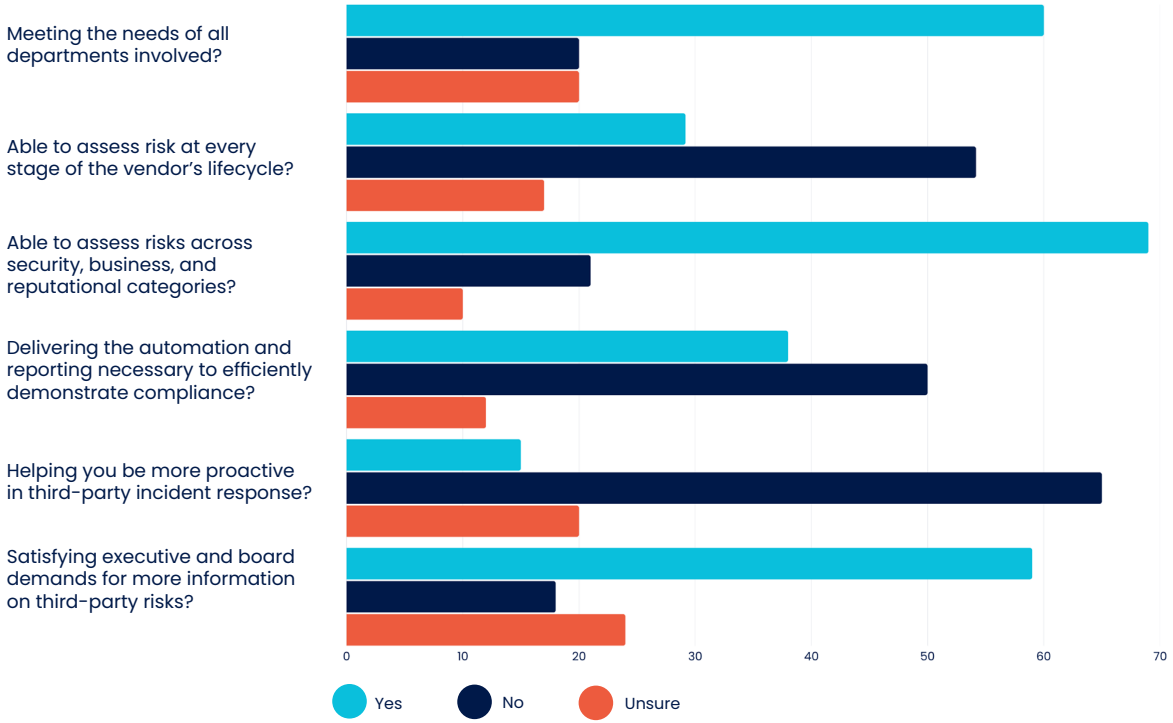
Manual Methods Undermine Insight and Agility

Despite rising risk complexity, 41% of programs still rely on spreadsheets, with 65% lacking confidence in incident response readiness and only 29% able to assess risk across the full vendor lifecycle.

Practitioners crave actionable insights to address key risks proactively and demonstrate compliance, but manual methods and disparate tools are thwarting success.

While 60% of respondents report that their current method of assessing third-party risk is meeting the needs of all departments involved, this satisfaction starts to steadily decline when asked whether they can assess risk at every vendor lifecycle stage, have the necessary tools to demonstrate compliance, and – most notably – how prepared they are for incident response.

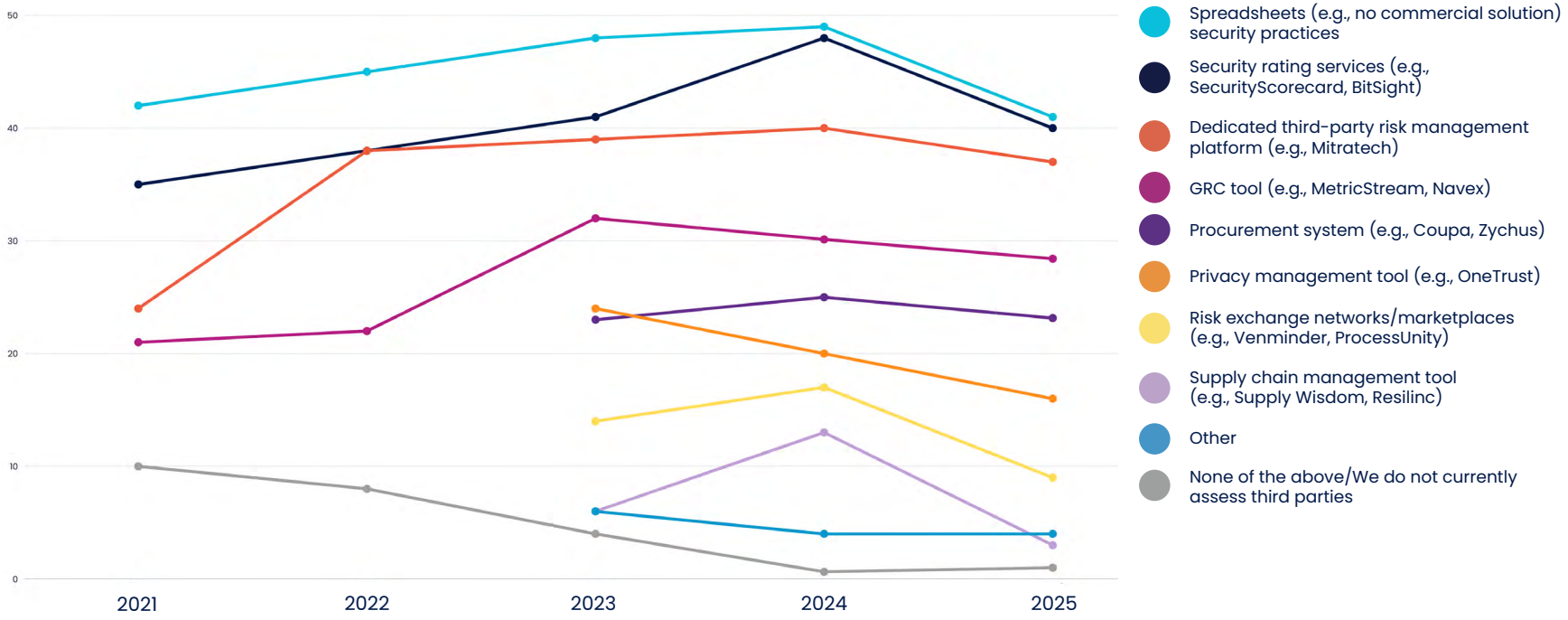
Is your current TPRM method:



Third-party data breach risks steadily remain a top concern for third-party risk management programs. Simultaneously, programs feel unprepared to address incident response. 65% of respondents are not confident in their current TPRM approaches to address incident response proactively. Additionally, 54% of respondents are not confident in their program's ability to assess risk across the vendor lifecycle. This is unsurprising when we consider that 41% of programs still report using spreadsheets to assess third parties.

A closer look at the approaches most organizations implement for assessing third parties reveals a fairly even distribution across various solution types, possibly due to organizations leveraging a combination of risk tools that may or may not function well together.

How do you currently assess your third parties?



What are the top concerns facing your organization regarding its usage of third parties? Rank them from 1 (most important) to 4 (least important).

1	**35.8%**	A data breach or other security incident due to poor vendor security practices
2	**24.1%**	A legal, reputational, or financial problem with a supplier
3	**20.8%**	An audit finding related to a third party
4	**19.3%**	A supply chain disruption due to a supplier/vendor/third-party failure

In the last year, has your organization experienced:

- A software supply chain attack? **11.58%**
- A legal or financial problem? **12.63%**
- A supply chain disruption? **12.63%**
- An audit finding? **25.26%**
- A data breach or other security incident? **33.68%**
- None of the above? **44.21%**

FINDING 5

AI Introduced With Caution Into the Ecosystem

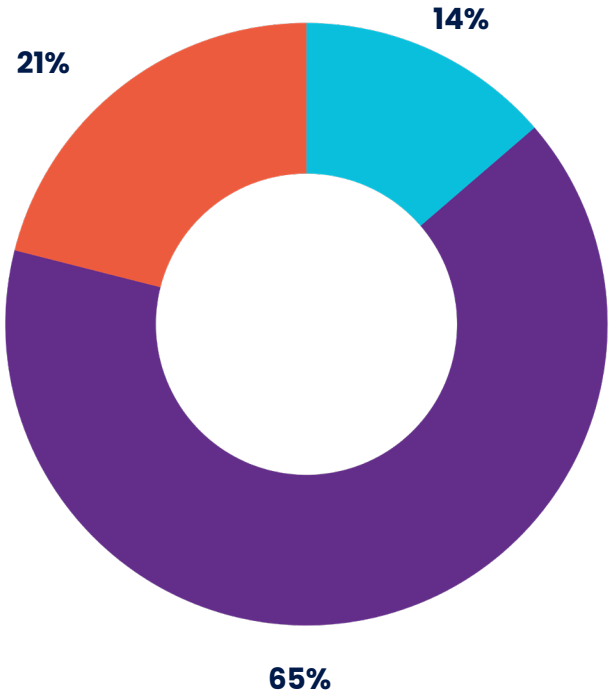
Although 65% of programs are exploring AI and nearly 14% are actively using it, concerns around data security, bias, and oversight persist — yet the lack of an AI strategy dropped significantly from 49% to just 12%.

AI-enabled solutions have advanced significantly over the past year, and the ecosystem is taking notice. Solutions are offering more sophisticated applications for artificial intelligence, and programs are exploring those use cases to address industry gaps.

Today, 65% of TPRM programs are actively exploring AI use cases, and nearly 14% (13.68%) have already adopted AI into their workflows — a marked increase from just 5% the year prior.

TPRM programs are increasingly (but cautiously) adopting AI-enabled solutions to streamline processes, enhance risk insights, and drive more value from risk management efforts. Risk managers recognize the benefits of efficiency while also identifying key risks that serve as barriers to implementation.

Is your organization currently leveraging AI in its third-party risk management program?



However, not all species thrive immediately upon introduction. For many, the rewards of AI remain speculative. In fact, 21.05% of respondents have no plans to implement AI, citing deep-rooted concerns about the reliability and safety of this emerging tool. Issues such as data security, algorithmic hallucinations, and the absence of human oversight represent serious threats to the balance of the risk ecosystem.

Much like environmental stewards worry about genetically modified organisms or invasive species, **TPRM professionals are scrutinizing the "nuts and bolts" of AI** — seeking assurance that it will enhance, not disrupt, the delicate systems they manage. Indeed, data privacy concerns loom large, especially as AI-specific legislation gains momentum. This is reflected in the 50% of respondents reporting increased involvement of data privacy teams in TPRM programs — a sign that this domain is becoming central to how organizations approach both AI and third-party risk.

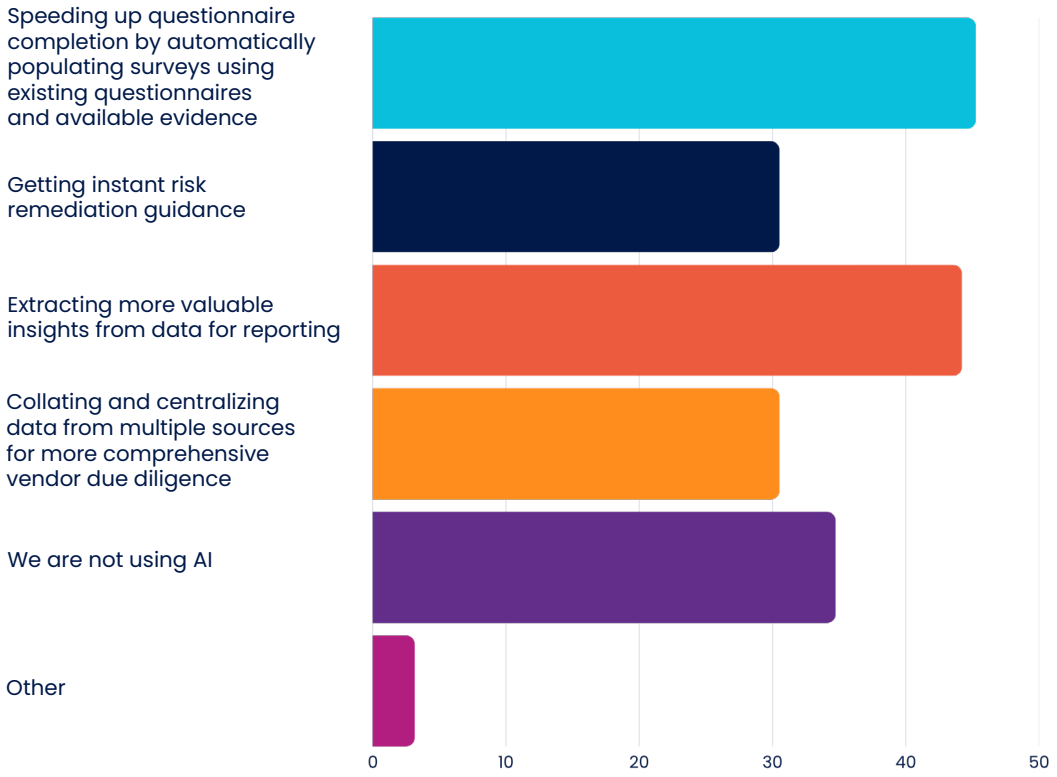
Importantly, the resistance to AI is evolving. While last year's most cited barrier was a lack of organizational strategy (49%), that number dropped sharply to 12% in 2025. This suggests that many organizations are now laying the groundwork to responsibly integrate AI into their ecosystems.

In nature, adaptation is the key to survival. As TPRM teams continue to explore AI, they are learning to do so with both optimism and caution — seeking to harness its benefits while ensuring that the broader ecosystem remains stable, secure, and sustainable.

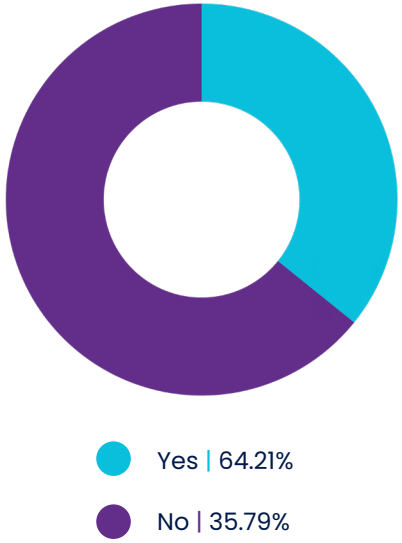
What is your most significant concern with using AI for third-party risk management in 2025?

31.58%	Data security risks
27.37%	Trusting AI to make decisions with minimal human oversight
18.95%	Risks of bias or hallucination
11.58%	No organizational strategy for AI
5.26%	Lack of transparency in algorithm models
4.21%	Regulatory scrutiny
1.05%	Possibility of job loss to AI

What are your goals with AI in your TPRM program?



Are you planning to implement a new or augment/replace an existing third-party risk management solution within the next 12 months?



Looking Ahead: A Future of a Balanced, Connected Risk Ecosystem

The overarching narrative of the 2025 study is one of convergence – fragmented, resource-depleted systems can't weather the regulatory storms or technological evolution that lie ahead.

Risk, Compliance, and Infosec teams are increasingly aligned, with a slow but visible shift toward shared ownership of risk data and program responsibilities. Organizations recognize that siloed risk management cannot keep pace with today's rapid pace of change and are beginning to adopt a more unified approach.

The findings highlight both the urgency and the opportunity in modernizing TPRM. Organizations recognize the need to evolve in order to meet regulatory expectations, secure vendor ecosystems, and gain meaningful insights into risk. It will require adopting smarter tools, integrating AI thoughtfully, and breaking down internal silos — so the path forward demands connected, coordinated, and resource-equipped TPRM programs.

Best-Practice Recommendations

Based on the findings from the Mitratech 2025 TPRM Study, here are five recommended best practices to help organizations cultivate a healthier, more resilient third-party environment — one that can withstand disruption, support growth, and adapt to constant change.

1. Establish Cross-Functional Governance for TPRM

Form a centralized **TPRM** steering committee that includes representatives from Risk, Compliance, Procurement, IT Security, and Legal. Define shared goals, standardized processes, and data ownership protocols.

Only 25% of programs are highly coordinated. A governance model ensures shared accountability, minimizes silos, and enhances visibility across the vendor lifecycle — particularly important when departments own different parts of the vendor relationship (e.g., procurement vs. risk oversight).

2. Operationalize AI with Caution and Clarity

Pilot AI-driven tools in low-risk use cases first (e.g., automating document classification or summarizing risk reports) and establish clear governance around AI transparency, data security, and oversight.

While 65% are exploring AI, only 14% have adopted it, and concerns around data integrity and hallucinations remain. A thoughtful implementation strategy builds trust in **AI outputs** and paves the way for scalable adoption.

3. Prioritize Resource Optimization Through Smart Automation

Conduct a strategic review of current manual processes and identify where **automation and AI** can deliver measurable efficiencies, such as pre-populating assessments, centralizing vendor data, or providing real-time risk scoring.

With nearly 70% of teams understaffed and only 40% of vendors being actively managed, risk managers need to "do more with less." Automation can alleviate assessment bottlenecks, reduce administrative burden, and free up personnel for higher-value activities.

4. Deepen Compliance Integration to Meet Evolving Regulatory Demands

Formalize compliance involvement in vendor risk assessments by integrating regulatory frameworks (e.g., **GDPR**, **DORA**, **Quebec Law 25**) directly into due diligence workflows and monitoring.

Compliance team participation grew from 42% in 2023 to 88% in 2025, with regulatory scrutiny being the top driver of change. Embedding compliance into TPRM processes ensures programs are audit-ready and resilient to legislative shifts.

5. Develop a Multi-Tiered Risk Assessment Approach

Adopt a tiered **risk assessment** model that categorizes vendors by risk level and applies proportionate due diligence. Combine traditional methods (e.g., questionnaires) with dynamic intelligence sources (e.g., security ratings, threat intel, and financial health indicators).

Despite the increased complexity of risk, many organizations still rely heavily on spreadsheets and disparate tools. A tiered, tech-enabled approach improves lifecycle coverage, increases assessment throughput, and surfaces critical risks more reliably.

Discover How Mitratech Can Help You Restore and Protect Your TPRM Ecosystem

Schedule a Demo ▶

Let's cultivate a safer, smarter, more sustainable environment for your extended enterprise.

About Mitratech

Mitratech has a 35-year history as a leader in providing technology and services that empower organizations to automate compliance, manage risks, increase efficiency, control costs, and scale for the future.

With an increase in remote and dispersed workforces, emerging technology, and rapidly changing regulations, teams across legal, risk, and human resources (HR) are collaborating now more than ever. Mitratech has emerged as the only partner delivering fully automated compliance and transparency across these three critical operational functions.

Mitratech serves over 24,000 organizations worldwide, spanning more than 160 countries.

For more information, please visit: **www.mitratech.com.**

MITRATECH

CONTACT US

info@mitratech.com
www.mitratech.com

Mitratech US
+1 (855) 462.6448

Mitratech UK
+44 (800) 368.9334