NCONTRACTS | venminder

State of Third-Party Risk Management Whitepaper 2025

Table of Contents

Executive Summary

The 2025 Venminder State of Third-Party Risk Management Survey offers a comprehensive look at how organizations are navigating the complexities of third-party risk today. Now in its ninth year, this survey dives deep into current practices, challenges, compliance drivers, and the tangible benefits of robust third-party risk management (TPRM) programs.

With input from a diverse range of industries — including financial services, fintech, retail, healthcare, insurance, IT, and more — the survey reflects organizations of all sizes, from small businesses with fewer than 100 employees to industry giants with over 5,000 employees. Conducted between November 2024 and January 2025, the survey leveraged email, social media, and Venminder's Third Party ThinkTank community to reach participants. Responses were kept anonymous to ensure honest and candid feedback, providing authentic insights into the state of third-party risk management today.

Highlights

The Rise of the Hybrid TPRM Model
The hybrid model has become the most popular TPRM operating model, with 52% of respondents using it, up 41% from the previous year. This shift indicates a maturing understanding of third-party risk management complexities.

Managing More Vendors Than Ever
Organizations are managing more vendors than ever, with a notable increase in programs handling 101-300 vendors (from 23% to 28%) and those with over 1,000 vendors (from 16% to 18%) – likely due to increased use of technology and expanding definitions of a third party.

TPRM Staffing Struggles to Keep Pace
Despite managing more vendors, TPRM staffing has not increased proportionally. Programs with 1-2 full-time employees rose from 43% to 48%, while those with 6-10 FTEs dropped significantly (from 10% to 4%).

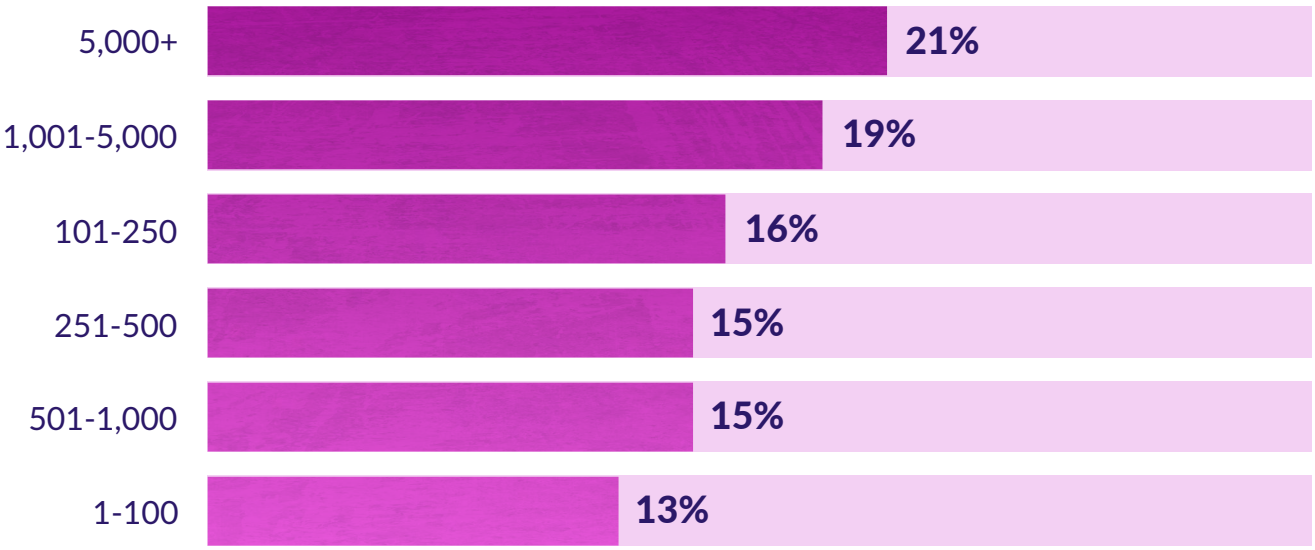
Shift Toward Dedicated TPRM Tools
The use of dedicated TPRM software platforms has increased by 19%, with 64% of respondents now using such tools. Manual methods like Excel/Google Sheets have decreased by 29%.

TPRM Programs Are Becoming More Mature
A majority of respondents (83%) consider their TPRM programs established to varying degrees, with 22% in the Optimizing phase, 22% Managed, and 39% Implemented but needing improvement.

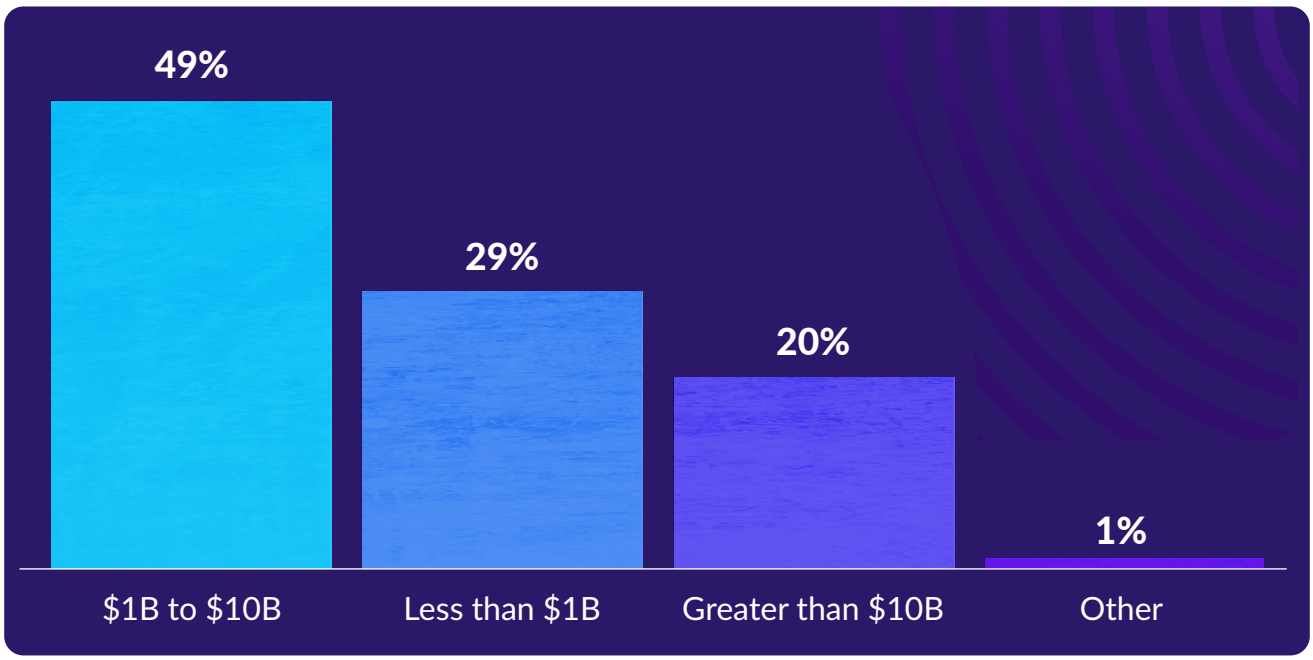
Rising Focus on Vendor Cybersecurity and AI Risks
Cybersecurity attacks on vendors remain a top concern, with 49% of organizations experiencing incidents in 2024. Additionally, there is growing attention to managing vendor AI risks, with a significant decrease in organizations not monitoring AI usage (from 37% to 23%).

About the Respondents

How many employees do you have?



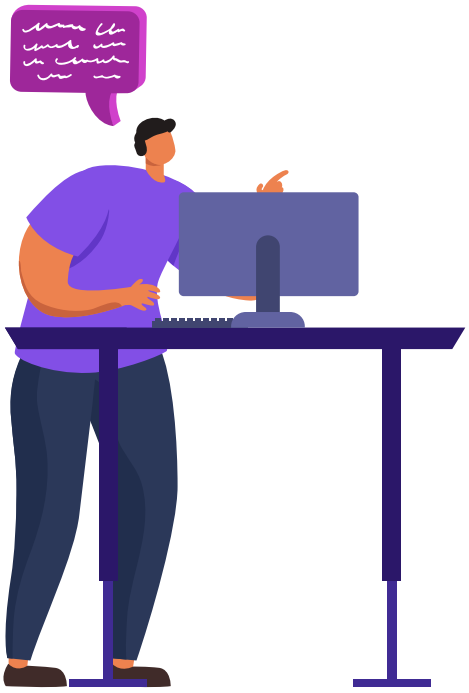
What is your asset size (if applicable)?



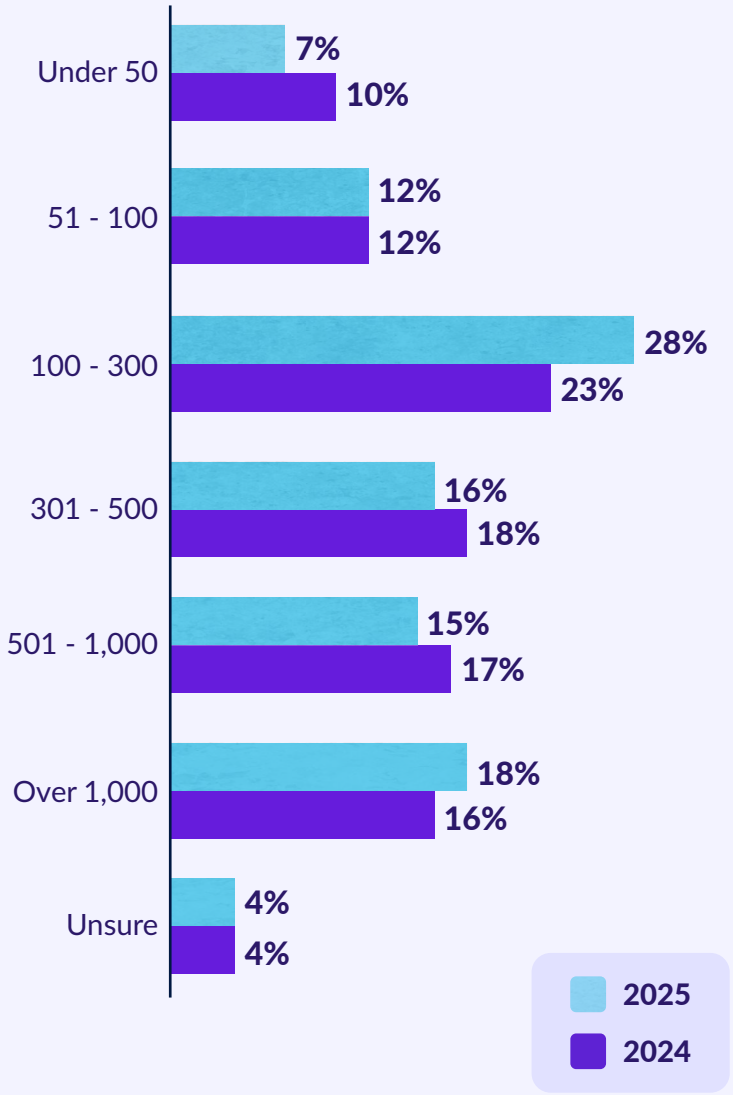
What Do TPRM Programs Look Like Today?

Organizations are managing more vendors than ever before — even as TPRM staffing shrinks.

Respondents with between 101-300 vendors in their TPRM program increased from 23% to 28% between 2024 and 2025 with a 30% decline in organizations managing fewer than 50 vendors (from 10% to 7%). Meanwhile, there was a 16% increase in programs with 1,000 or more vendors (16% to 18%).



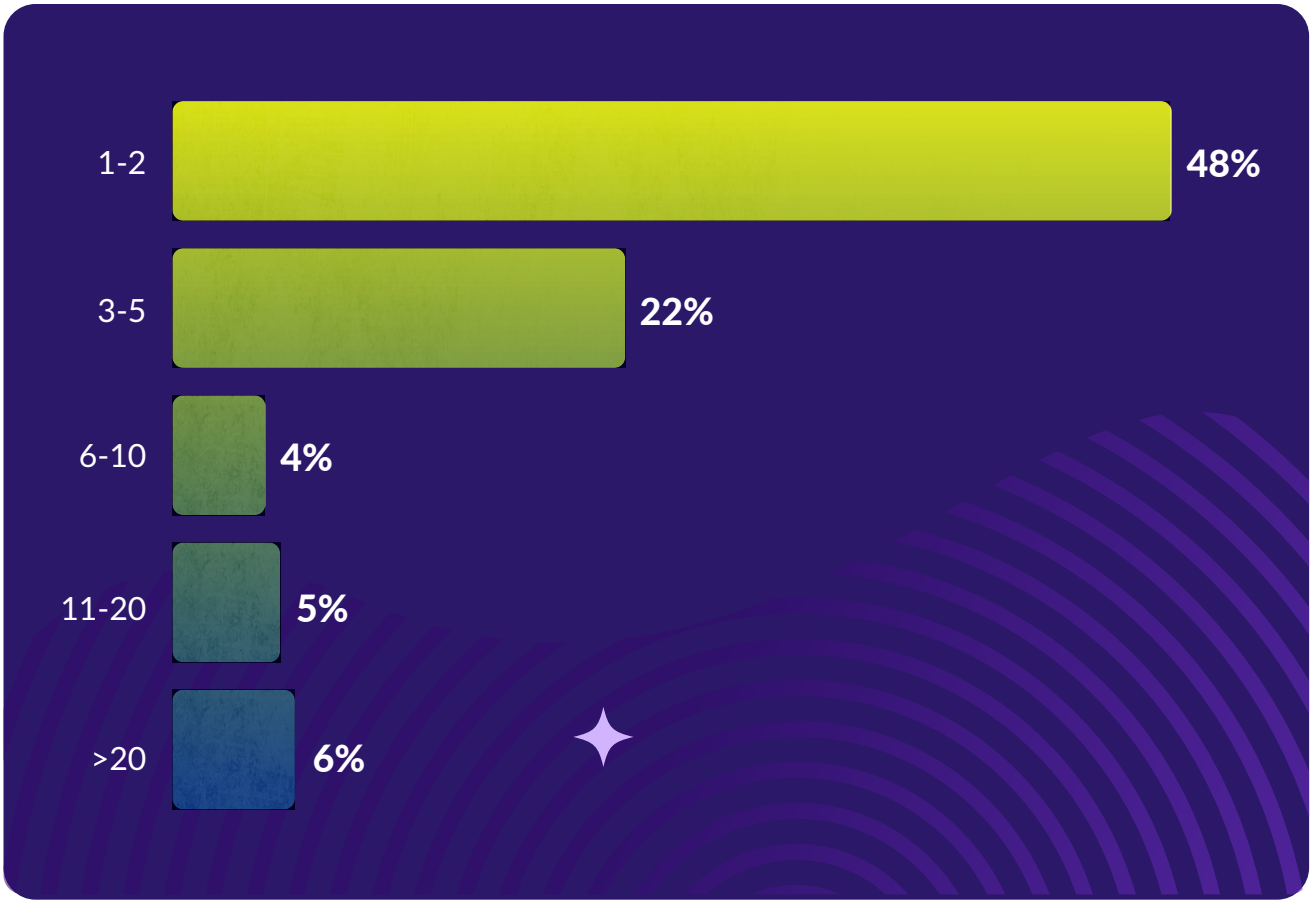
How many total vendors are included in your third-party risk management program?



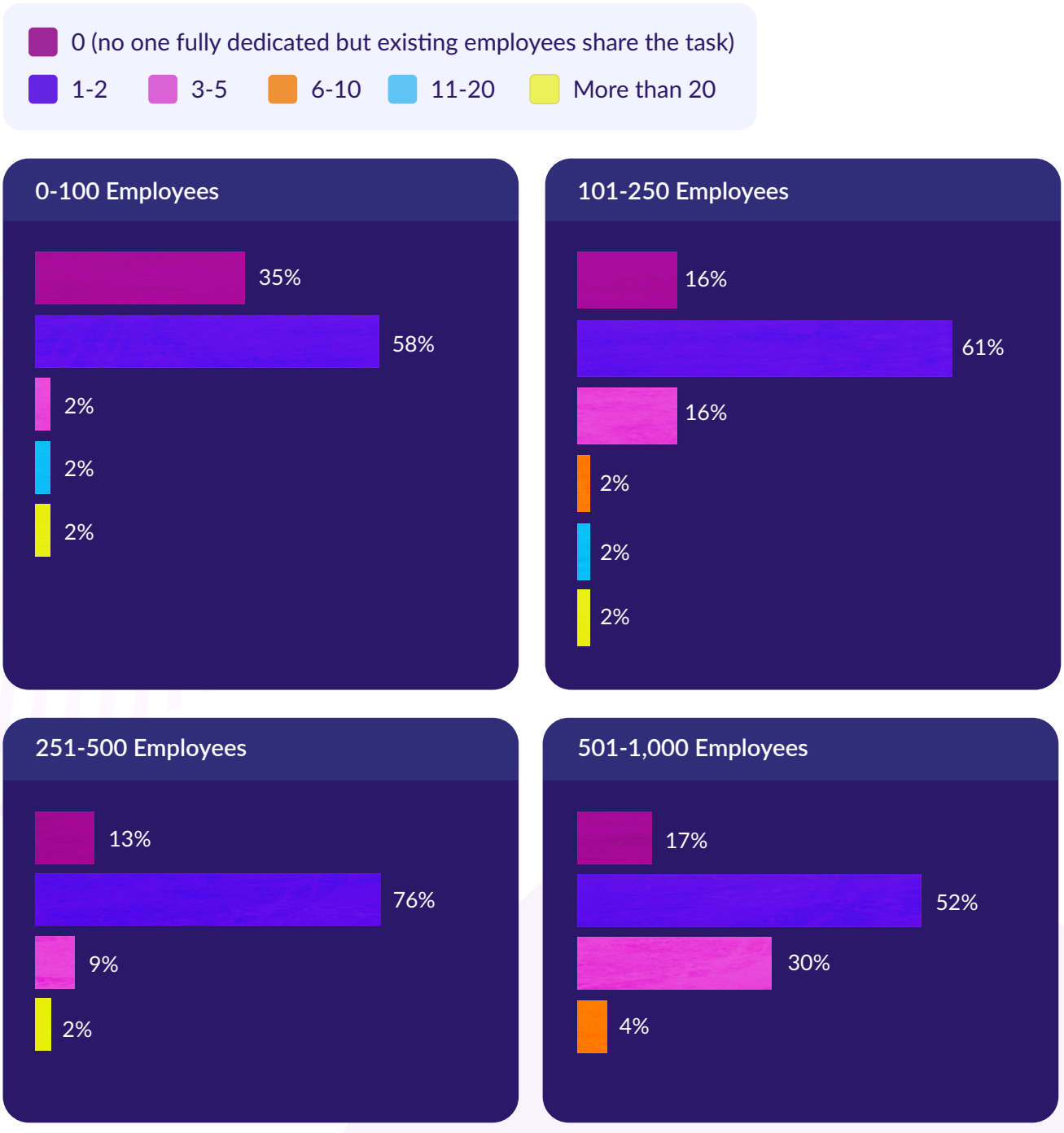
While managing more vendors might lead a financial institution to increase its TPRM staffing, that hasn't been the case. The number of programs with 1-2 full-time staff employees (FTEs) rose from 43% to 48% while the number of programs where there is no single staff person dedicated to TPRM remained steady. Why the increase? It's likely some of it stems from a significant decrease in the number of programs with 6-10 FTEs, which dropped 60% (from 10% to 4%).

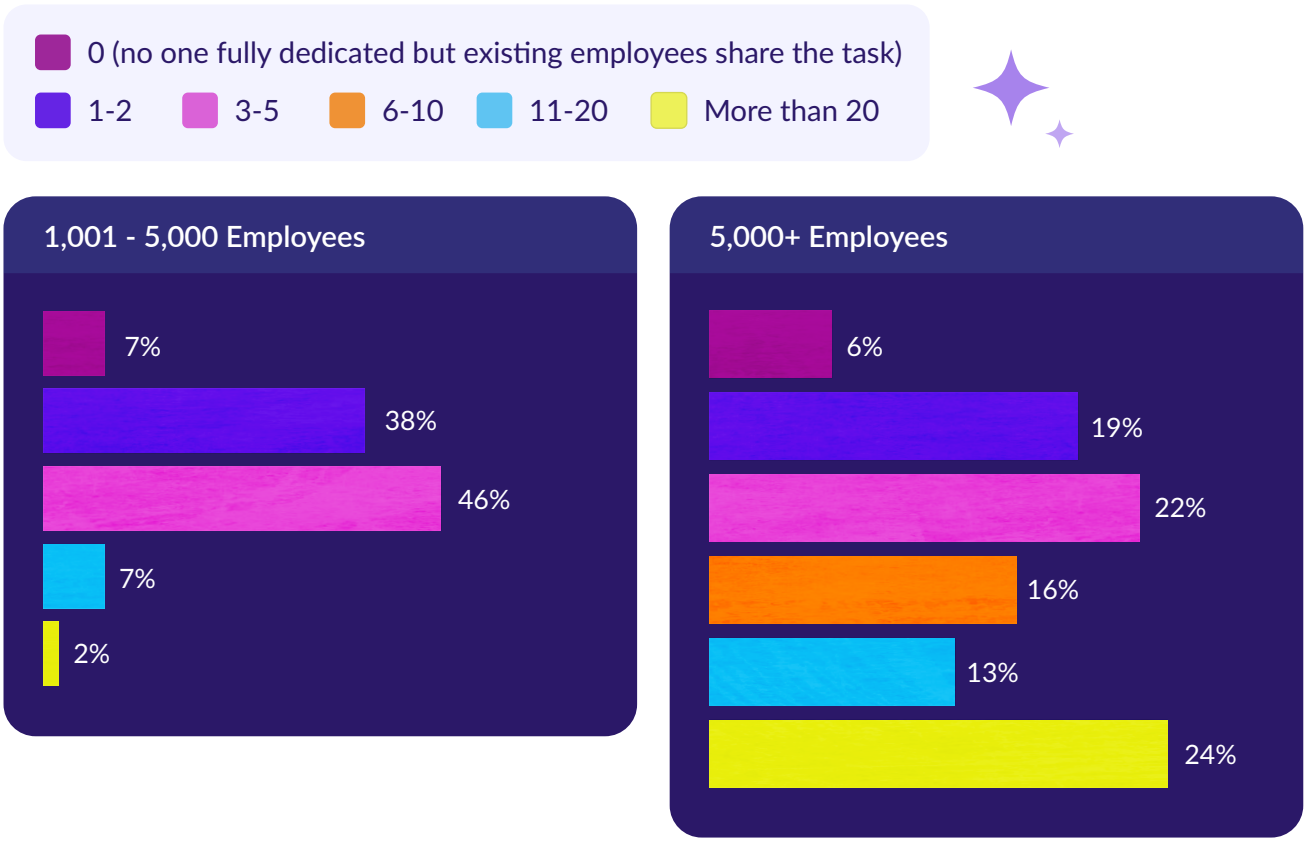
Either these programs found ways to make their TPRM program more efficient with automated tools or economic pressures forced them to reduce headcount. The decision likely depends on each organization's third-party risk tolerance.

How many full-time employees are dedicated to your third-party risk management program?



Breakdown of TPRM FTEs by Organization Size

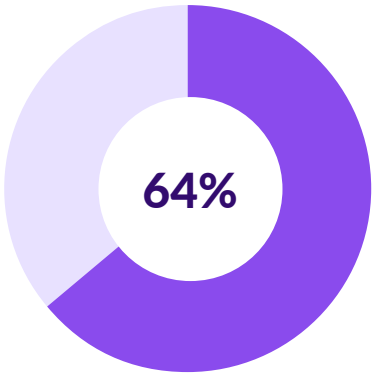




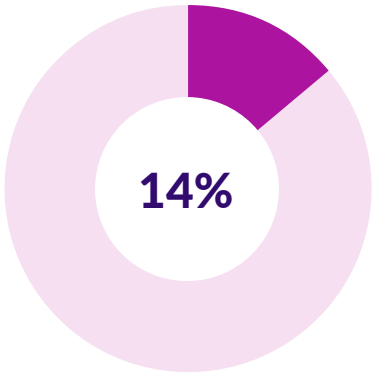
Organizations continue to embrace tools to manage vendor risk. Most respondents (64%) use a dedicated TPRM software platform — an increase of 19% from last year — or a TPRM module inside of an ERM or GRC platform to manage third parties (14%).

A few holdouts still rely on manual methods for TPRM, though these numbers continue to fall. Just 12% use Excel/Google Sheets to manage third-party risks — a 29% decrease from last year. A small fraction use SharePoint (3%) or an Access Database (1%) for TPRM (each down a percentage point from 2024).

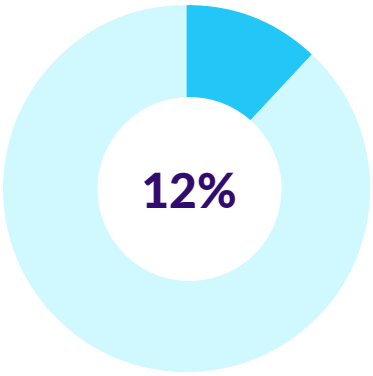
What is your primary tool for managing vendor risk?



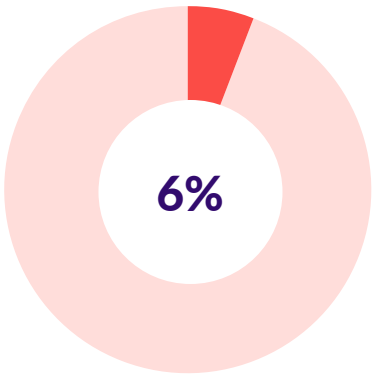
Dedicated vendor risk management software platform



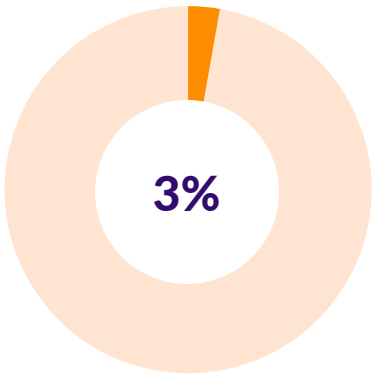
Vendor risk management module inside of an ERM, GRC, or other platform



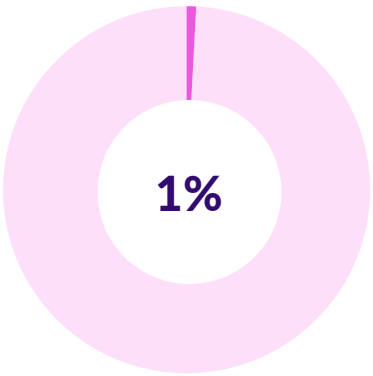
Excel/Google Sheets



Other



SharePoint

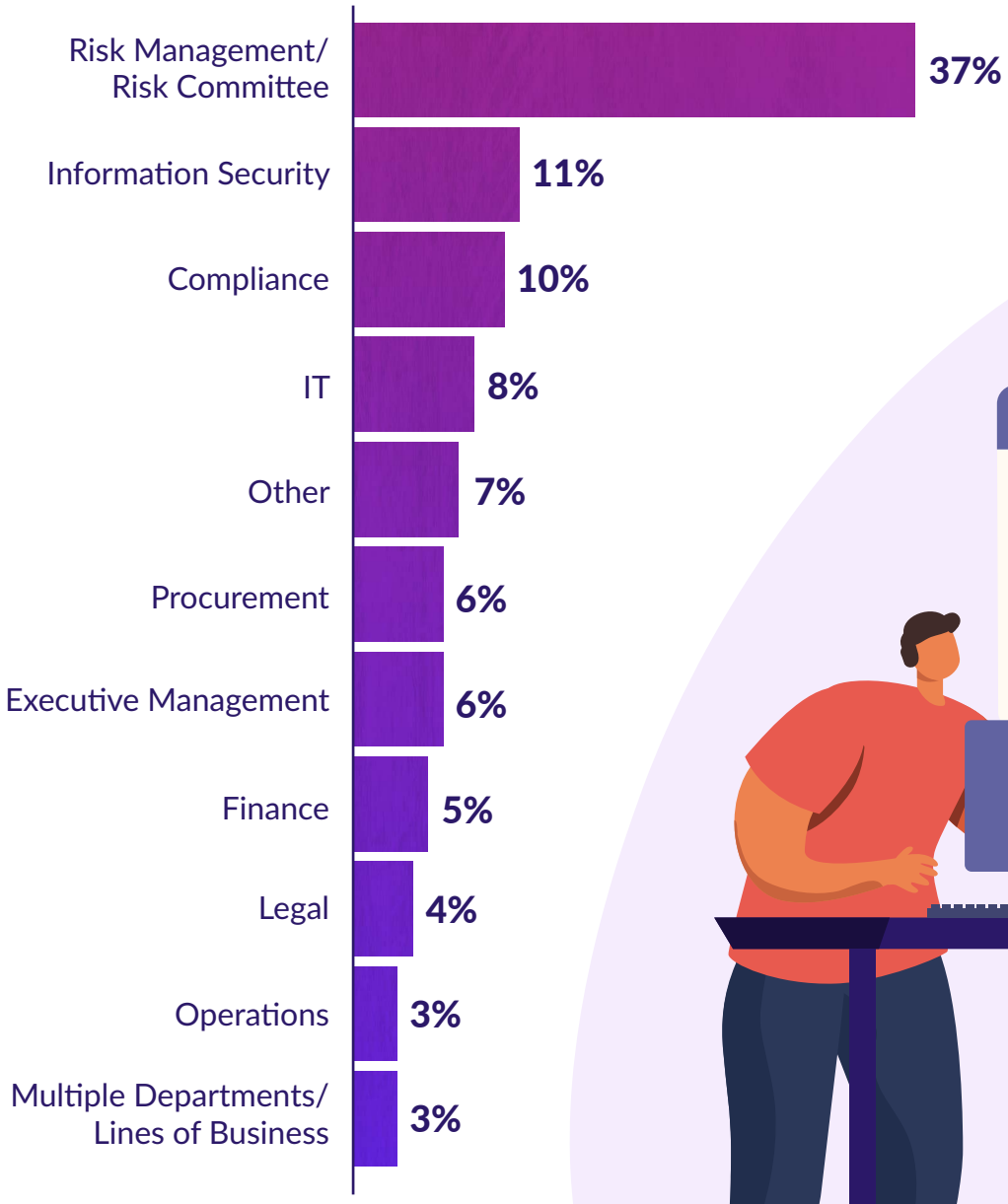


Access Database

Nearly half (47%) of organizations follow the best practice of having their TPRM program report to Risk Management or Compliance. Aligning TPRM with these risk-focused departments enhances visibility, boosts credibility, and fosters stronger internal compliance.

Other arrangements can also support effective TPRM implementation and oversight, depending on the institution's size, structure, and strategic priorities. For example, 19% of TPRM programs report to either information security or IT.

What department does TPRM report to?



TPRM Program Maturity

This year saw a significant shift in TPRM operating models. Most TPRM programs choose from one of four operating models:

Hybrid: Dedicated TPRM team responsible for framework, task assignment, quality control, and oversight. Vendor risk and performance management are the responsibility of vendor owners across the organization.

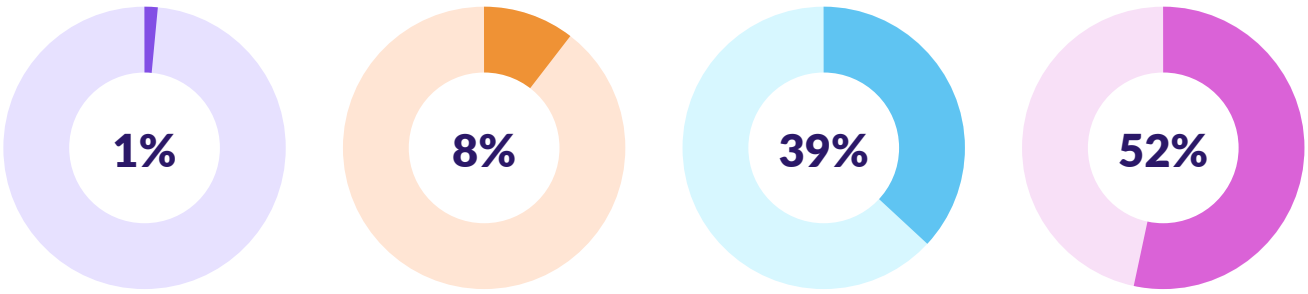
Centralized: All TPRM functions, including risk and performance management, are handled by the same team.

Decentralized: No dedicated TPRM team, responsibilities for TPRM are distributed across the organization.

Totally outsourced: All TPRM functions and tasks are performed by external vendors.

While the centralized model reigned in years past, 2025 saw the hybrid model take the lead. Surging up 41% in the past 12 months, more than half of respondents (52%) now use the hybrid model with 39% using the centralized model (down 25% year over year).

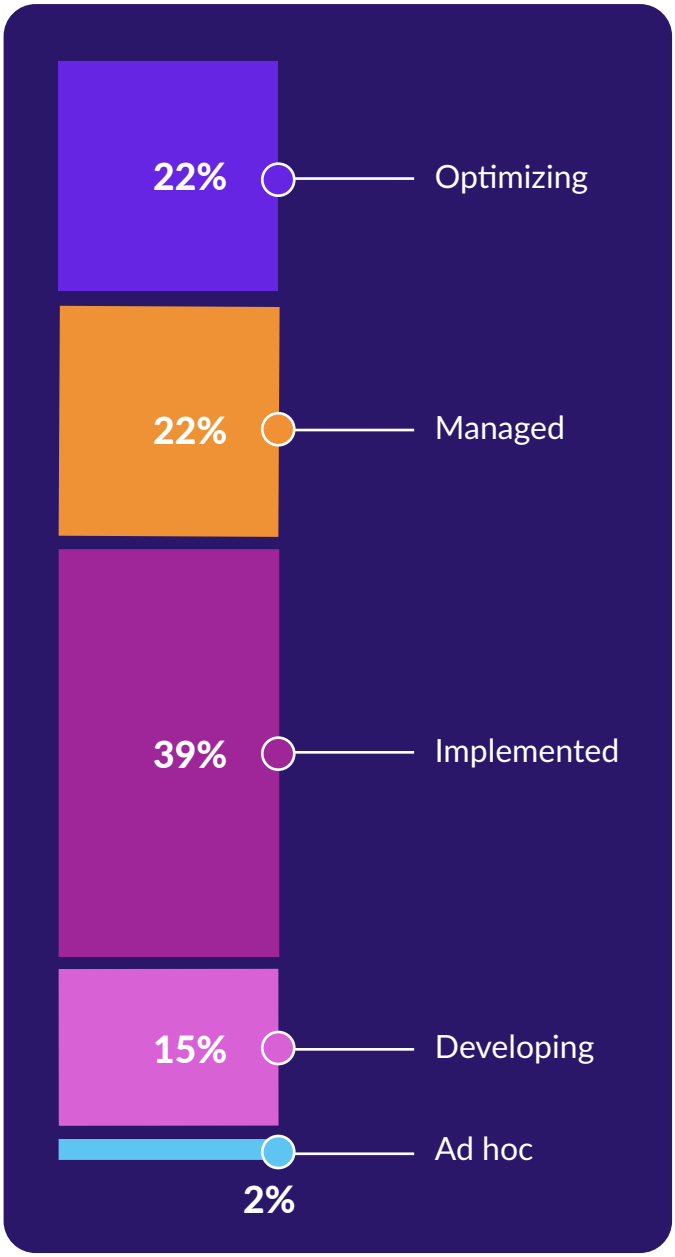
What operating model do you use for your TPRM program?



This is a sign that TPRM is maturing at organizations, as it reflects a deeper, more comprehensive understanding of the complexities involved in managing third-party relationships. An advantage of the hybrid model is that while one team maintains overall responsibility for the program, individuals with direct, day-to-day interactions with vendors are also actively involved, ensuring accountability and nuanced oversight across the TPRM process. This model works best when supported by vendor risk management software, which facilitates the interdepartmental collaboration essential to its success.

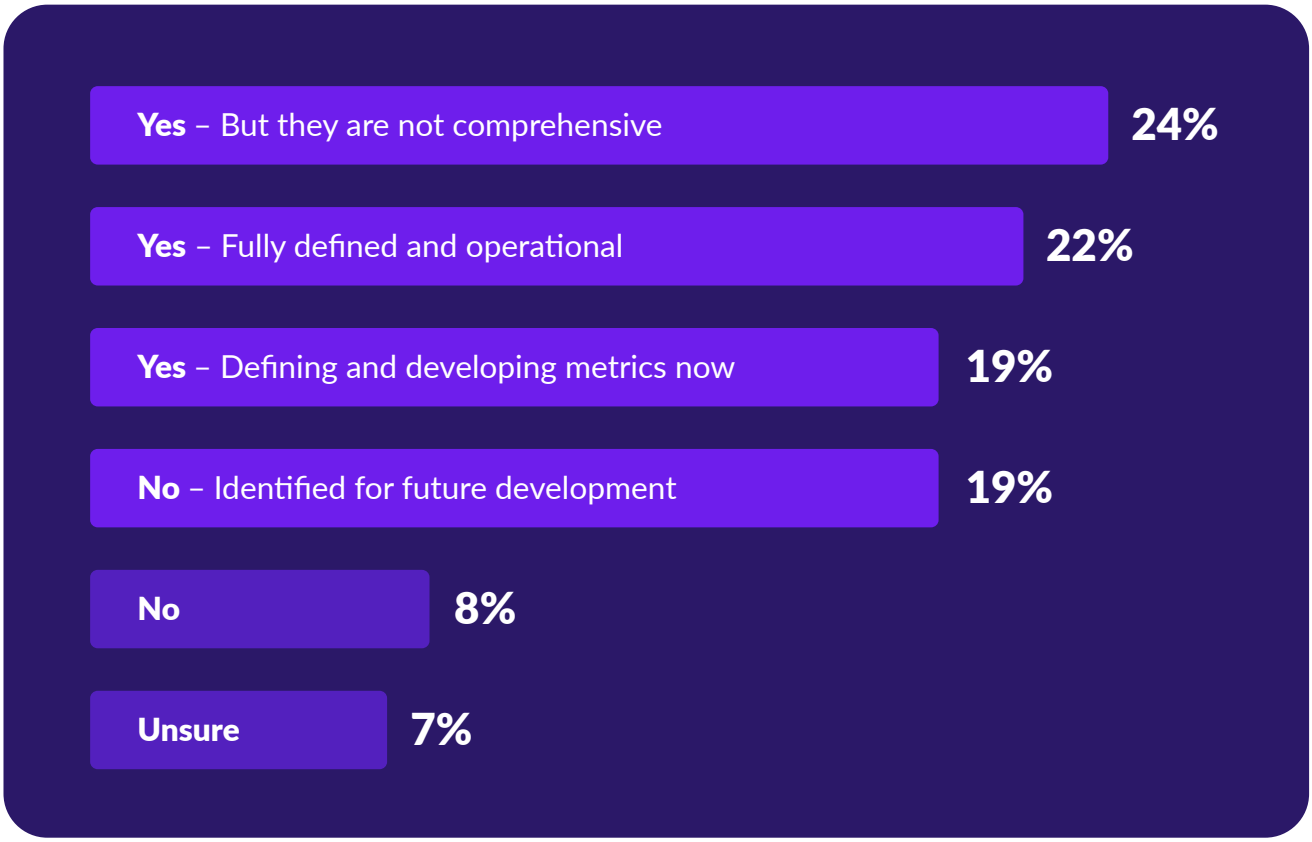
That aligns with how organizations view the maturity of their program. The vast majority of respondents (83%) say their TPRM program is established — though to varying degrees. There are the Optimizers (22%) who say their TPRM program is fully integrated into their overall risk management framework and continuously monitored and updated. Another 22% say their TPRM program is Managed, fully established and implemented, while the largest number (39%) say their program is Implemented but requires improvement.

What stage of development is your third-party risk management program at?



TPRM metrics are another measure of an organization's TPRM program maturity, offering insights into the program's health, stability, and effectiveness by identifying strengths, gaps, and areas in need of improvement. The survey revealed a split among organizations.

Does your organization have defined metrics to measure the health, stability, and effectiveness of the TPRM program?



Twenty-two percent of respondents said their metrics are fully defined and operational, much like the 22% who say their TPRM program is in the Optimizing phase. Another 24% said they have metrics, but those metrics aren't comprehensive. Other organizations have more work to do — 19% are currently defining and developing metrics and another 19% have identified metrics for future development. Only 8% said they currently have no metrics — a 3% decrease from 2024's survey.

While there's been progress, it's clear that most organizations will have to improve their metrics as they mature their programs.

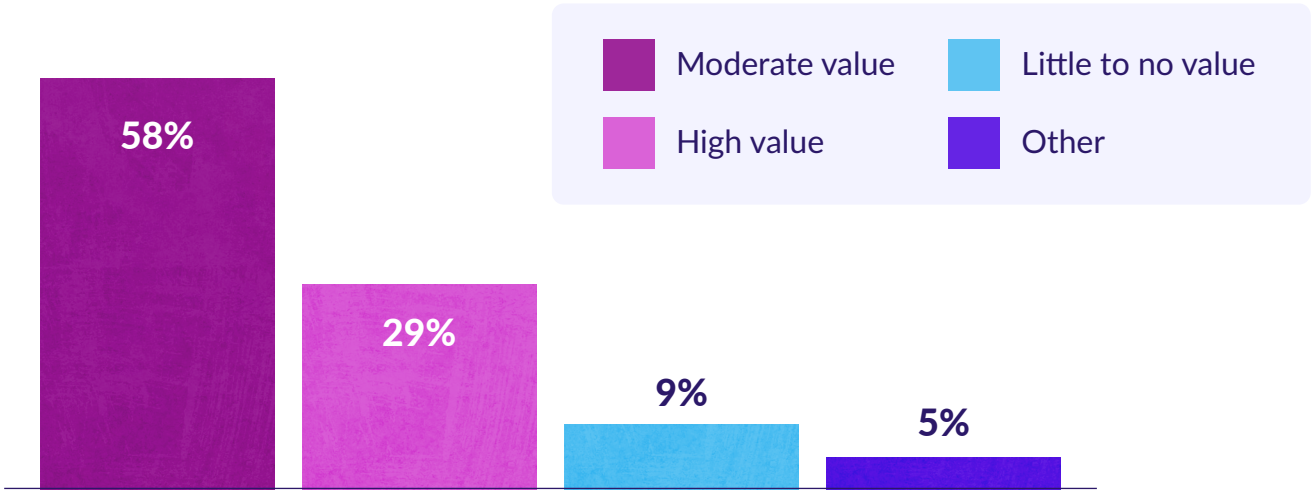
Organizational Perception of TPRM

An organization's approach to third-party risk management (TPRM) significantly impacts the program's effectiveness. Senior management and the board of directors play a crucial role in setting a tone from the top that underscores the importance of TPRM and its value to the organization, fostering support across all levels.

The vast majority of organizations (87%) believe there is value in investing in TPRM activities. TPRM is considered a valuable investment throughout the organization at 29% of organizations. Another 58% say TPRM provides a moderate return on investment (ROI), seeing value in regulatory compliance, cost savings, operational resilience, and contract management. For example, one respondent offered that the biggest benefit has been contract management, saying "This year alone we've saved about 20K in canceling auto renewals on contracts we didn't want or need as we started the cancel process within the time frame allowed."

Only 9% believe that TPRM is solely a regulatory requirement with little value.

Does your organization believe there's a return on investment/value from investing in TPRM activities?



Organizations have different reasons for investing in TPRM. Meeting regulatory requirements is the primary reason for TPRM at 61% of responding organizations. This is particularly common in the financial services industry, which must follow stringent requirements for TPRM, and those subject to rules like the European Union's (EU) Digital Operational Resilience Act (DORA), which took effect this year and includes several TPRM requirements. Enforcement actions for failing to comply with TPRM regulations can be costly and damage reputations.

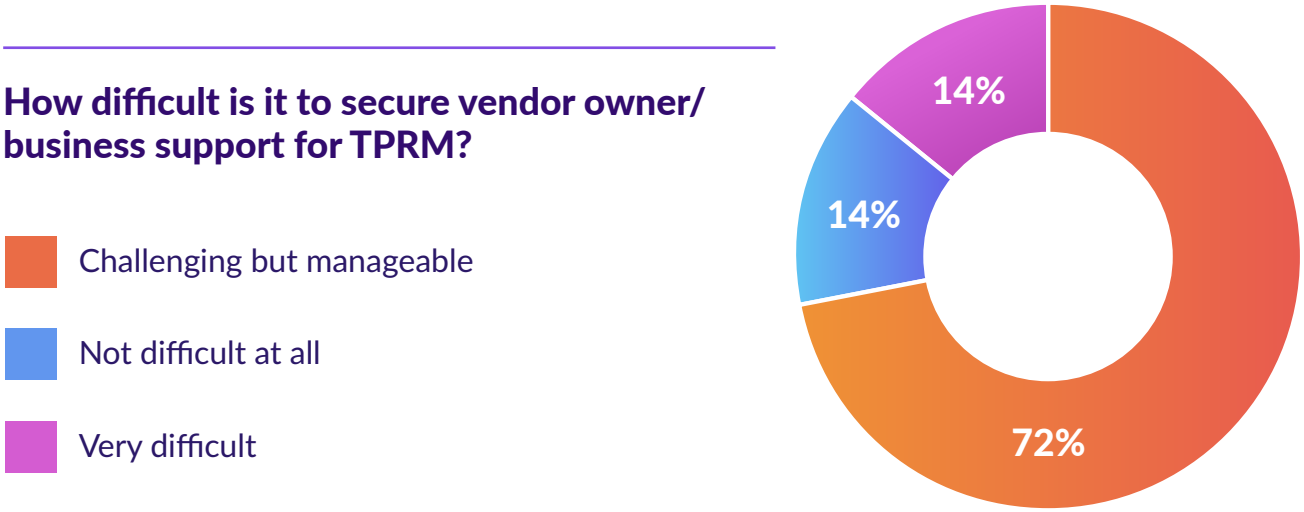
Avoiding third-party cybersecurity incidents was also a major reason. (See section on **Vendor Cybersecurity Risk & Artificial Intelligence** for more information.) Other respondents were primarily concerned with protecting their brand and reputation, while others want to align with industry best practices. Controlling vendor costs pushed past managing vendor performance to claim the fifth spot.

What are your primary reasons for doing third-party risk management?

1. Meet regulatory requirements
2. Avoid third-party cyber incidents
3. Protect our brand and reputation
4. Align with industry best practices and standards
5. Control vendor costs
6. Manage vendor performance

While most respondents (72%) reported that securing vendor owner or business unit support for their TPRM program was challenging but manageable, 14% found it very difficult. In good news for TPRM, 14% indicated it wasn't difficult at all, up 17% from last year.

How difficult is it to secure vendor owner/ business support for TPRM?



TPRM Best Practices

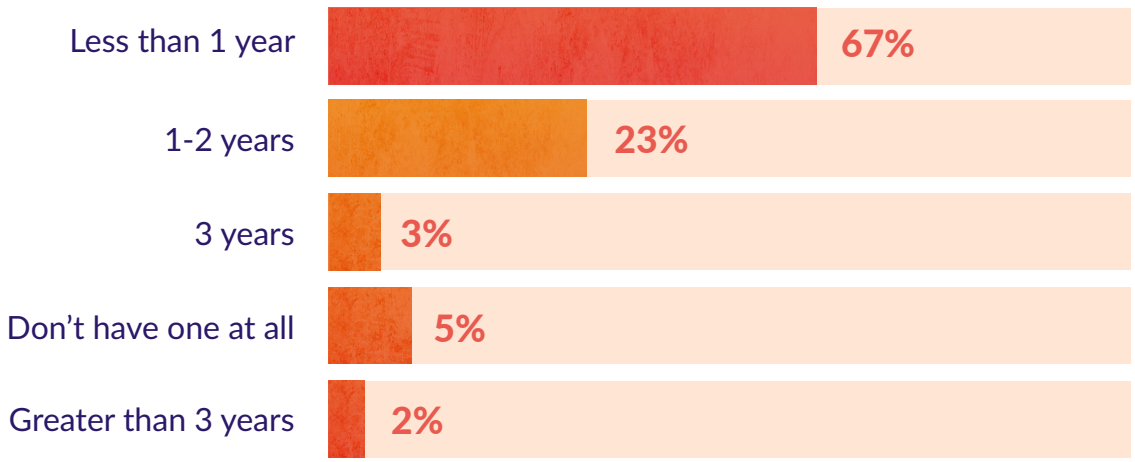
We asked respondents about their practices for common TPRM activities to gauge how many align with best practices and regulatory requirements. It's encouraging to see that many are adhering to these recommendations, which play a critical role in strengthening their TPRM programs and safeguarding their organizations from external risks.

TPRM Policy Updates

An updated TPRM policy document is essential to ensure it reflects the program's current practices and aligns with regulatory requirements. Sixty-seven percent of respondents reported updating their policy within the last year, while 23% updated it within the last 1–2 years.

It's important for organizations to regularly review policy documents, especially when there are changes to regulations or best practices. For example, U.S. bank regulators released the Interagency Guidance on Third-Party Relationships: Risk Management in 2023, prompting many banks to revisit and refine their processes in 2024. This focus on compliance with evolving standards reinforces the importance of maintaining flexibility in vendor risk management practices to adapt to regulatory changes.

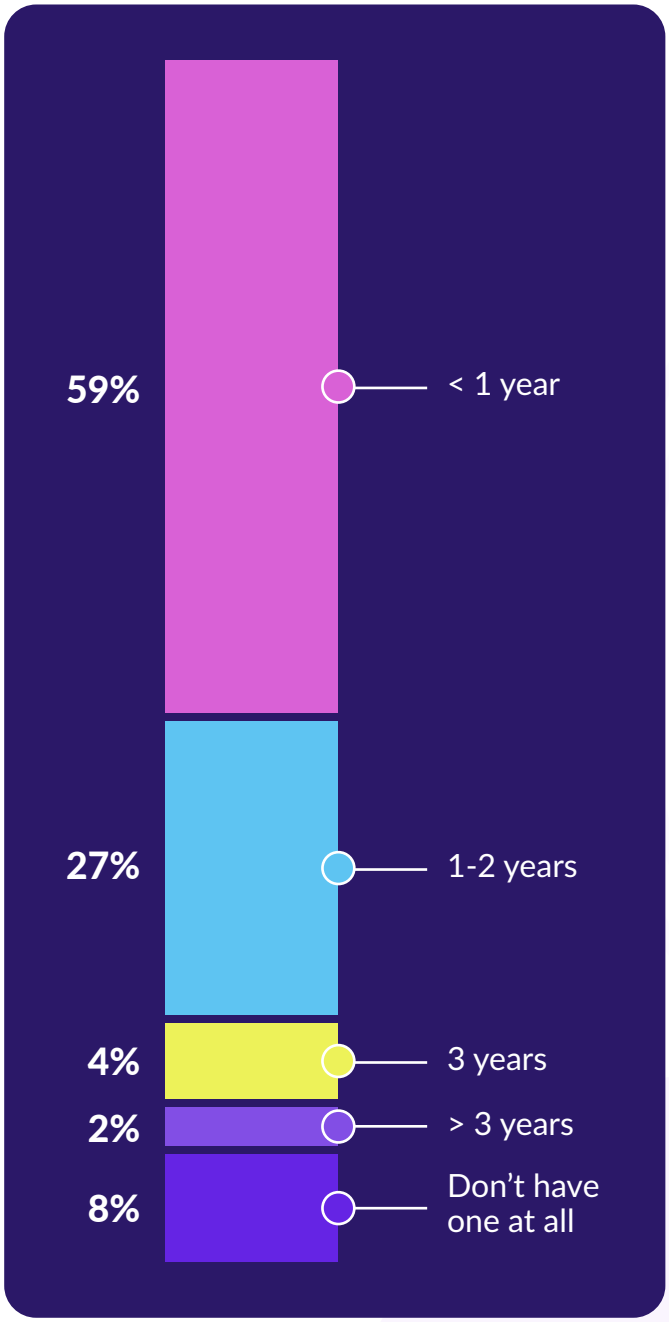
How recently have you updated your third-party risk management policy document?



Inherent Vendor Risk Assessments

Inherent risk assessments have been almost universally adopted, with 92% of respondents completing them — and 59% updating them within the last year and 27% within the last 1–2 years. As risks evolve and emerge over time, it's essential to capture those changes in the inherent risk assessment.

How recently have you updated your inherent vendor risk assessment?

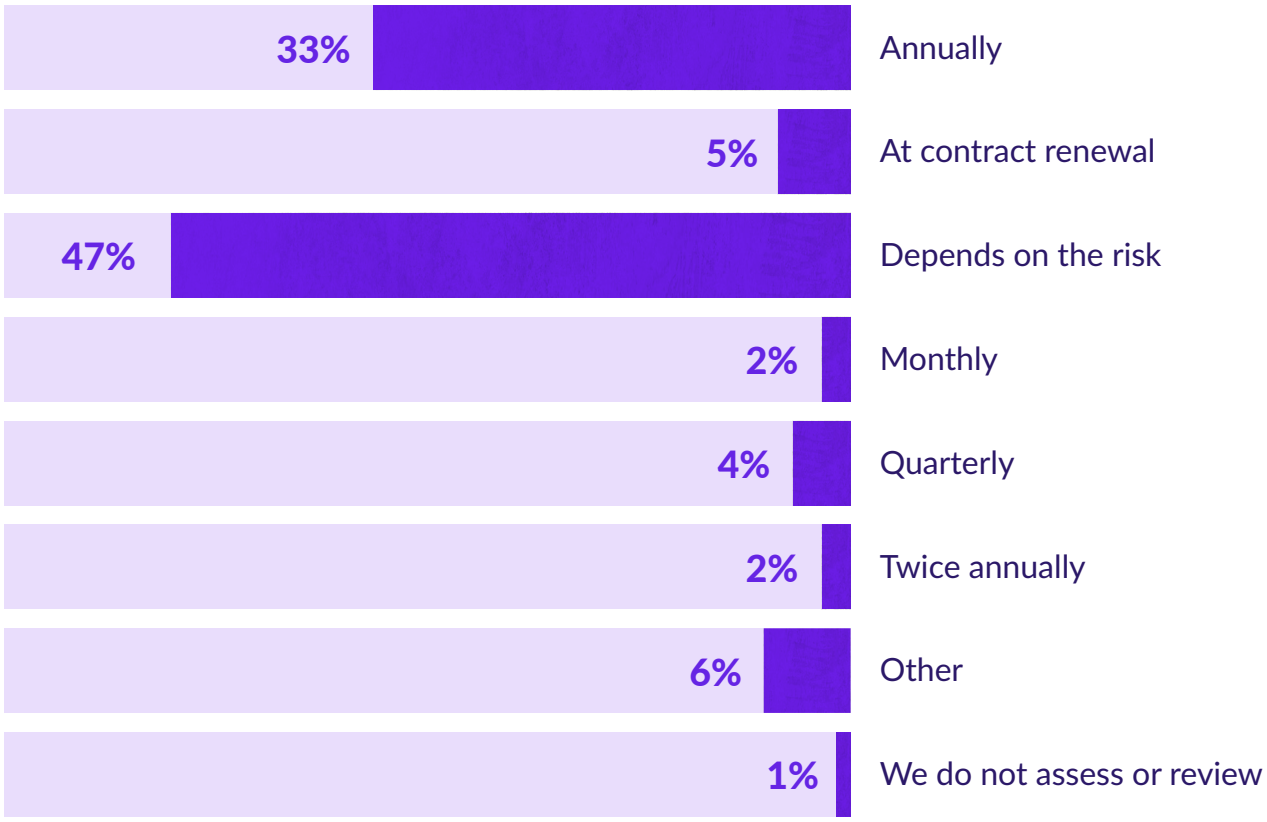


Vendor Risk Profiles and Documentation

We asked organizations how often they review and reassess vendor risk profiles and documentation. Following best practices, 47% said the frequency depends on the vendor's risk — a 5% drop from last year. This decrease is likely offset by a 5% increase in respondents who reported conducting reviews and reassessments annually (33%).

While annual reviews can provide a consistent cadence, aligning review frequency with a vendor's risk profile is widely regarded as a best practice. It ensures that higher-risk vendors receive the necessary scrutiny, while lower-risk vendors don't divert resources unnecessarily. A balanced approach is key to an effective TPRM strategy.

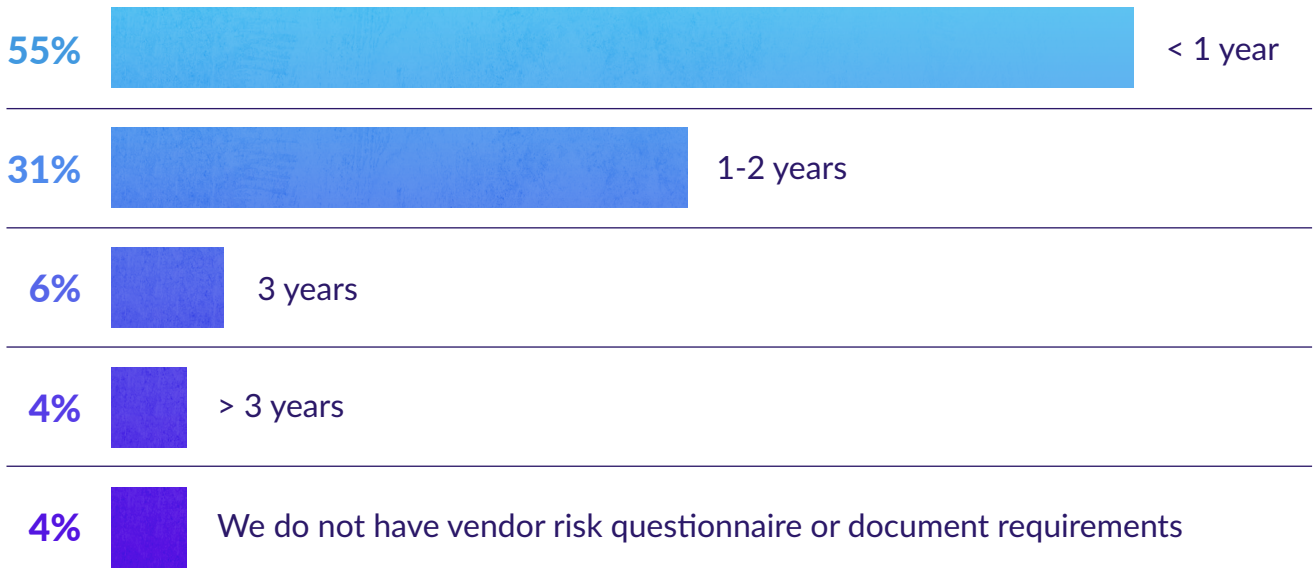
How often are you reassessing and reviewing vendor risk profiles and documentation?



Vendor Risk Questionnaires and Due Diligence Document Requirements

Fifty-five percent of respondents updated vendor risk questionnaires and due diligence document requirements within the past year and 31% reported updating them within the last 1–2 years. Just 4% don't have a vendor risk questionnaire or document requirements.

How recently have you updated your vendor risk questionnaire and due dilligence document requirements?



Regular updates help organizations stay responsive to evolving risks and compliance expectations, reinforcing the foundation of an effective TPRM program.

TPRM Oversight and Challenges

When it comes to the challenges of vendor risk management, due diligence documentation is hands-down respondents' number one daily frustration. Almost half (45%) said getting timely, accurate documentation from vendors ranks among their top three daily challenges. Another 20% cited analyzing those documents — including SOC reports, financials, and contracts — and 19% said tailoring due diligence requests for each vendor. These challenges highlight why outsourcing aspects of vendor management, like documentation collection and analysis, is becoming an increasingly popular solution for organizations seeking to streamline the process and reduce frustration.

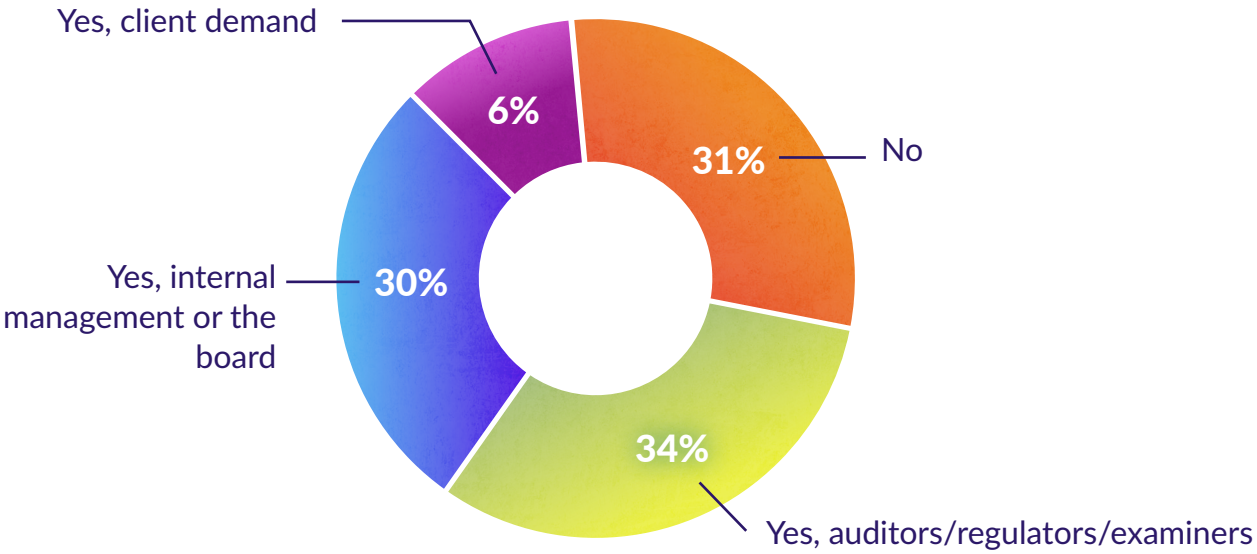
A close second is having the internal resources (33%) and time (27%) to effectively tackle TPRM. Automating the process (27%) and completing risk assessments (24%) also ranked high. These findings show that while automation can be a game-changer, it requires the right tools and approach to make it work seamlessly — another reason organizations are turning to trusted partners to fill resource gaps and simplify TPRM.

Top 5 TPRM Challenges

1. Getting the right documents from vendors
2. Having enough internal resources
3. Automating the process
4. Time management
5. Completing risk assessments

It's not surprising that these are stressors. Seventy percent of respondents are feeling pressure to improve their TPRM programs. This pressure comes from auditors/regulators/examiners (34%) and management and the board (30%). In some cases it stems from client demand (6%) — likely from growing awareness that most data breaches originate from third-party vulnerabilities.

Are you feeling pressure to improve your third-party risk management program?



When it comes to exams and audits, more organizations report getting feedback on their TPRM programs. Just 14% said they had no comments on TPRM — down from 17% last year. Another 29% said regulators or auditors told them improvements were needed. Just 37% said all is well and there are no findings and 9% didn't have an audit or examination.

It shouldn't be a surprise that many are feeling pressure from regulators to improve. Several recent banking enforcement actions homed in on TPRM practices and banking as a service (BaaS) relationships. More privacy regulations passed in 2024, emphasizing the importance of protecting customer data — even in the hands of third-party vendors. Other global regulations took a close look at third parties and operational resilience.

During your last exam/audit, did your regulator/auditors provide feedback on your current third-party risk management program?

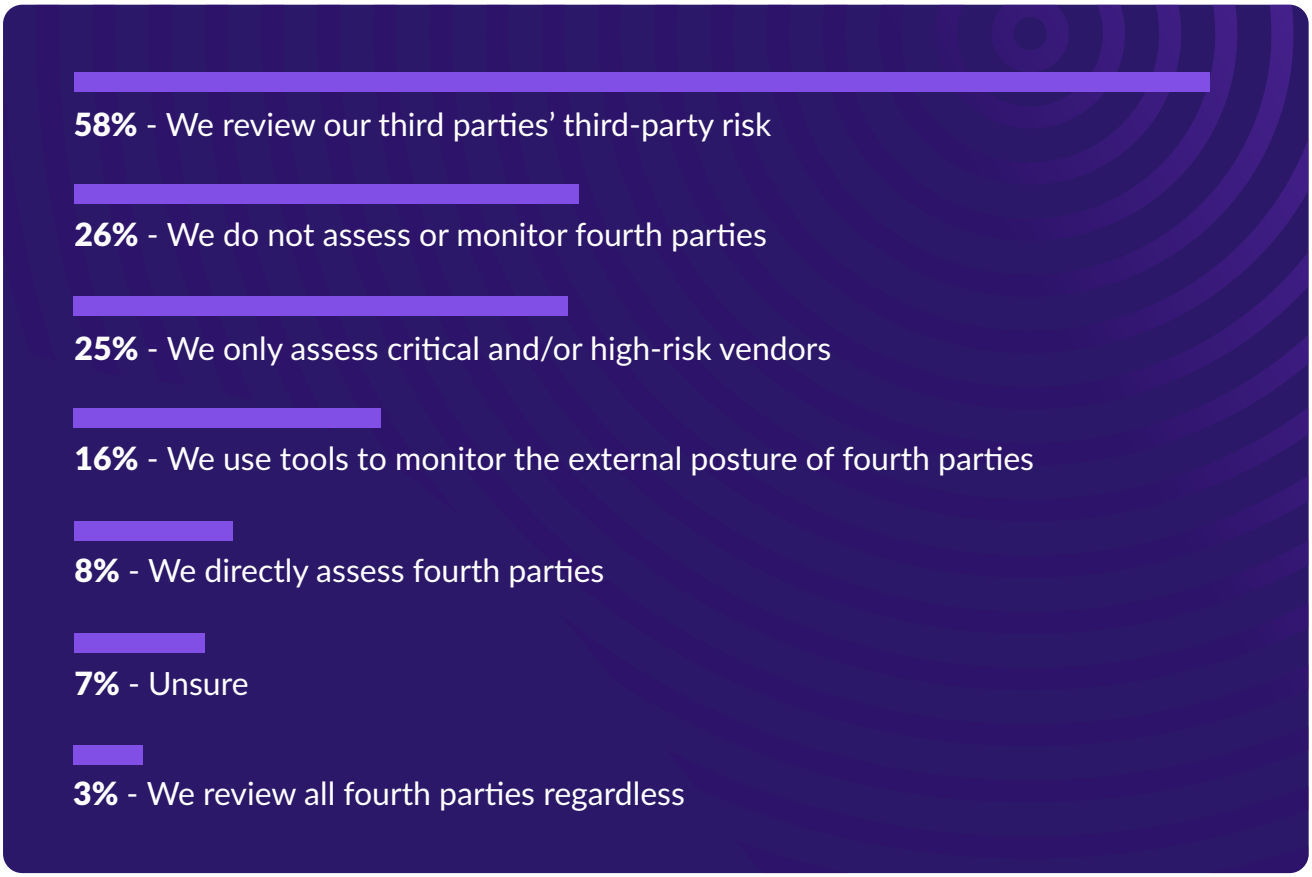
Fourth-Party Risks

Fourth-party risks are a growing challenge for organizations, demanding effective strategies to manage them. When it comes to oversight, organizations take a variety of approaches to tackle this critical issue.

According to our survey, 58% follow best practices by reviewing their third parties' risk management programs to ensure fourth-party oversight. Twenty-five percent said they focus on assessing or monitoring only critical or high-risk fourth parties, and 16% rely on tools to monitor the external posture of their fourth parties — an efficient way to keep tabs on risks without a direct contract.

That said, 26% of respondents admitted they don't currently assess or monitor fourth parties. While managing fourth-party risks can seem daunting, it's essential to protecting your organization and strengthening your overall vendor risk management strategy.

How does your organization review fourth-party vendors/subcontracts (your vendors' vendors)?



*Respondents were asked to select all that apply

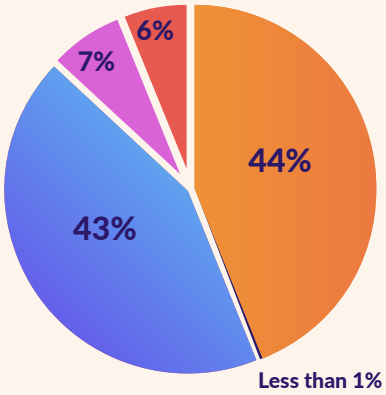
Vendor Cybersecurity Risk & Artificial Intelligence

When it comes to the TPRM risks organizations are most concerned about going into 2025, cybersecurity attacks aimed at vendors remains the top concern — and for good reason. Almost half of organizations (49%) experienced a third-party vendor cyber incident in 2024.

Among those that experienced a moderate-impact third-party cyber incident, two-thirds (66%) reported that monetary costs were one of the biggest impacts of the event in addition to reputation damage (50%) and regulatory scrutiny (33%). Many wrote in to share operational headaches such as system outages and slowdowns and the need to implement alternative systems and workarounds. Investigating the issue also proved cumbersome.

Even low-impact events caused monetary, reputational, and regulatory damage. One respondent shared, “While the incident did not have significant effects, the firm’s clients desired change from the vendor.”

Over the past 12 months, has your organization experienced a third-party cyber incident?



How long was the recovery process after the third-party incident?

64% - Less than 60 days

10% - 60-90 days

9% - 90+ days

1% - Recovery is still ongoing

16% - Unsure

Top TPRM Concerns

1. Increase in cybersecurity attacks at vendors
2. Use of artificial intelligence (AI) by our vendors
3. Pending or anticipated regulatory changes
4. Our vendors' operational resilience during an unexpected event

Vendor use of artificial intelligence is another top concern, with organizations allotting more vendor management resources to mitigating this risk. In 2024, 37% of organizations weren't managing AI risk. That number has fallen dramatically in 2025 to just 23% — a 38% decline.

Organizations are using or planning to use many of the tools in their TPRM arsenal to assess and monitor vendor AI risk. They are adding language to vendor contracts (40%), documenting risks (39%), and verbally communicating with vendors (38%). Contract management, vendor risk assessments, and speaking with vendors about how their AI use might impact an organization are essential for any organization that is worried about vendor AI risk — but there is a control for mitigating vendor AI risk that organizations have been slower to adopt: collecting vendor documentation.

Collecting documentation is critical to the due diligence process — an essential step in the vendor risk management lifecycle. Examples of documents that can help assess vendor AI risk include policies detailing how the vendor ensures ethical AI usage, accountability, and decision-making oversight and documentation offering insights into model development and training (i.e. data sources and quality standards), algorithmic decision making, and security.

How is your organization currently or planning to assess/monitor vendor usage of artificial intelligence (AI)?

Recommendations and Best Practices

8 TPRM Best Practices for 2025
(Aligned with Survey Takeaways)

1. **Evaluate Your TPRM Operating Model**
Consider whether your current operating model — centralized, decentralized, or hybrid — is meeting your organization's needs. As complexities in vendor risk management grow, evolving to a hybrid model may provide the flexibility and scalability required for effective oversight.

2. **Tie Oversight Frequency to Vendor Risk**
Follow best practices by reviewing and reassessing vendor risk profiles based on their risk level rather than a one-size-fits-all approach. This ensures high-risk vendors get the attention they require.

3. **Keep Your TPRM Policies and Procedures Up to Date**
Review your TPRM policy document annually — and when there is a major change in regulation or the risk environment — to reflect current practices.

4. **Stay on Top of Fourth-Party Risk**
Evaluate your third parties' risk management programs to ensure they are protecting your organization from fourth-party risks. This approach helps tackle the ongoing challenges of managing deeper supply chain risks.

5. **Strengthen Cybersecurity and AI Risk Oversight**
Cybersecurity attacks on vendors remain a top concern. Conduct in-depth assessments of vendors' security controls and monitor their use of AI to address emerging risks.

6. **Leverage TPRM Technology to Offset Vendor Growth**
With organizations managing more vendors than ever, ensure staffing levels and resource allocation keep pace to prevent gaps in oversight and program performance.

   Invest in TPRM platforms to streamline vendor management activities and do more with less. Reduce reliance on manual processes like spreadsheets to enhance efficiency — an approach more organizations are embracing.

7. **Implement Continuous Monitoring**
Regularly review vendor documentation and risk profiles to stay ahead of emerging risks. Automation and risk intelligence tools can enhance monitoring without overwhelming your team.

8. **Foster Program Maturity and Consistency**
Focus on moving your TPRM program toward the "Optimizing" phase by establishing consistent practices, closing resource gaps, and refining processes based on program reviews and external benchmarks.

About Venminder

Third-party risk management done right.

Venminder by Ncontracts is an industry-recognized leader of third-party risk management solutions. Dedicated to third-party risk, the solution is the go-to partner for software, high-quality assessments on vendor controls, certified subject matter expertise, and education.

The Venminder platform is used by more than 1,200 customers across a wide range of industries to efficiently execute their third-party risk management programs. As Venminder's solutions are designed to accommodate growth and various levels of program maturity, customers range in size from small to top Fortune 100 organizations.

Our offerings.

Software platform

Control assessments

Venmonitor

Request a demo

Connect with us.

LinkedIn

X

Facebook

Stay Updated on Third-Party Risk Management

- Attend a live webinar
- Get the weekly Third Party Thursday Newsletter
- Join the Third Party ThinkTank Community
- Read the latest articles
- Download free educational content

About Venminder

Venminder is a leading SaaS platform for third-party risk management for enterprise and wealth management businesses and is part of the Ncontracts suite of solutions. It is trusted by over 1,200 customers to streamline the entire vendor lifecycle — from onboarding to offboarding. Combining advanced technology with human expertise, Venminder empowers users to manage vendors, track contract data, perform due diligence, assess risks, monitor threats, and more.

Venminder also hosts Third Party ThinkTank, the largest online community dedicated to third-party risk management. For more information, visit http://www.venminder.com or follow Venminder on LinkedIn, X, Facebook, and YouTube.