The State of Third-Party Risk Management 2026

NCONTRACTS

ncontracts.com | 888.370.5552

Table of Contents:

Executive Summary

The 2026 State of Third-Party Risk Management Survey reveals an industry at a critical inflection point. Organizations are managing larger vendor inventories with leaner teams while confronting emerging risks like artificial intelligence (AI) that demand new approaches to vendor oversight.

This year's findings come from financial services professionals surveyed between November 2025 and January 2026. Respondents span all sizes, from small financial institutions with less than $250 million in assets to those with more than $10 billion in assets. Survey responses were kept anonymous to ensure candid feedback and authentic insights into the state of third-party risk management.

The data shows TPRM programs caught between technological advancements and resource limitations, where process maturity doesn't always result in confidence.

TPRM Programs Run Lean While Managing Hundreds of Vendors

Most TPRM programs operate with minimal staffing while managing substantial vendor portfolios. Nearly two-thirds (63%) run on just 1-2 dedicated employees, and another 13% have no dedicated staff at all. At the same time, over half (53%) manage 300+ vendors, creating ratios where individual professionals oversee 100+ vendor relationships.

No One Feels Confident Managing AI Risk — Not Even Large Organizations

Vendor AI risk is a top concern for financial institutions — but most don't have clear visibility into where that risk exists. In fact, 72% of institutions are only partially aware of which vendors are using AI. Not a single organization feels "extremely confident" managing AI-related risks. The majority feel either slightly confident (38%) or moderately confident (31%), but that number drops even further when you look at large organizations.

Boards and Executives Are Demanding TPRM Improvements, Not Just Regulators

Nearly three-quarters (73%) of organizations feel pressure to improve TPRM. Internal stakeholders apply as much pressure as regulators — 38% cite internal management/board pressure while 31% cite regulatory pressure. TPRM is a compliance and strategic imperative recognized by regulators and boards.

Spreadsheets Can't Measure What Matters

Organizations using TPRM software are better equipped to track program effectiveness. Excel users are twice as likely to have metrics that don't comprehensively measure program health. More tellingly, 23% of software users are actively developing new metrics compared to 0% of Excel users.

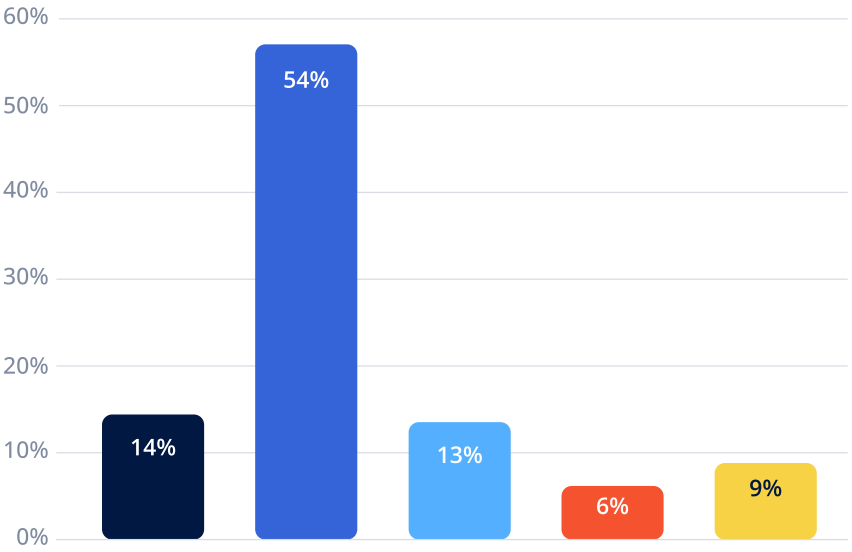
The Hybrid Model Dominates Because It Scales

The hybrid operating model — where a central TPRM team sets standards and coordinates oversight while business units maintain day-to-day vendor relationships — has become the dominant approach. Most organizations (60%) now use the hybrid model, up 15% from last year, and 84% of hybrid users have established programs at varying maturity levels. This shift away from centralized and decentralized models (which both declined) demonstrates organizations recognizing what scales.

Strategic Value Recognition Follows Program Investment

As TPRM programs mature, organizations increasingly recognize their strategic value. Among programs at the "Optimizing" stage, 26% view TPRM as high value throughout the organizations. Meanwhile, the percentage viewing TPRM purely as a compliance checkbox drops dramatically — from 67% at Ad Hoc to just 13% at Optimizing. Organizations that invest in building mature TPRM programs see the return on investment.

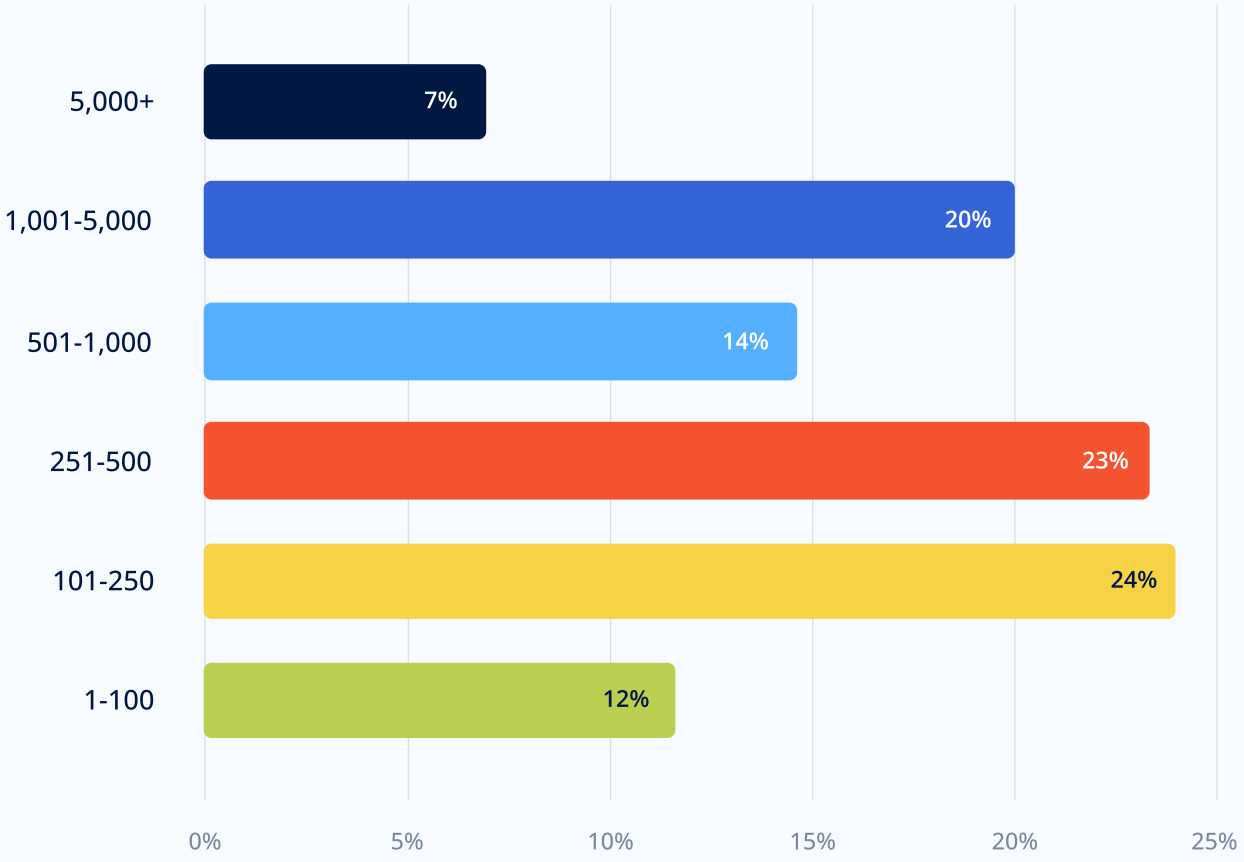
About the Respondents



What's your asset size (if applicable)?

- Greater than $10 billion in assets
- $1 billion to $10 billion in assets
- $500 million to $999 million in assets
- $250 to $499 million in assets
- Less than $250 million in assets

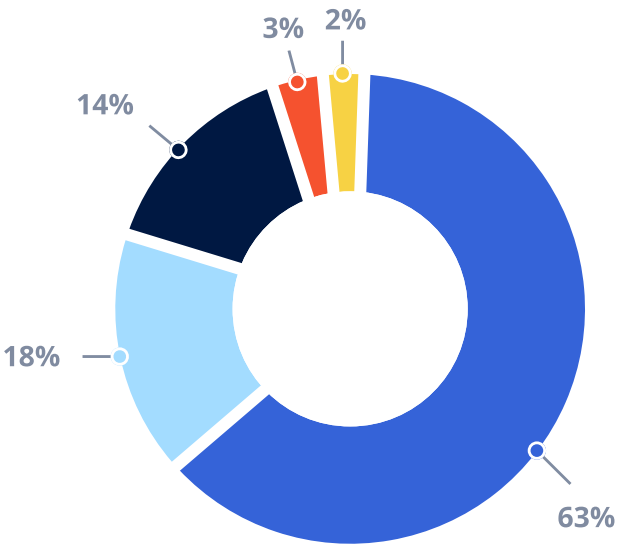
How many employees do you have?



TPRM Programs in 2026

TPRM programs are running lean: 63% operate with just one or two dedicated full-time employees, yet these small teams manage substantial vendor portfolios.

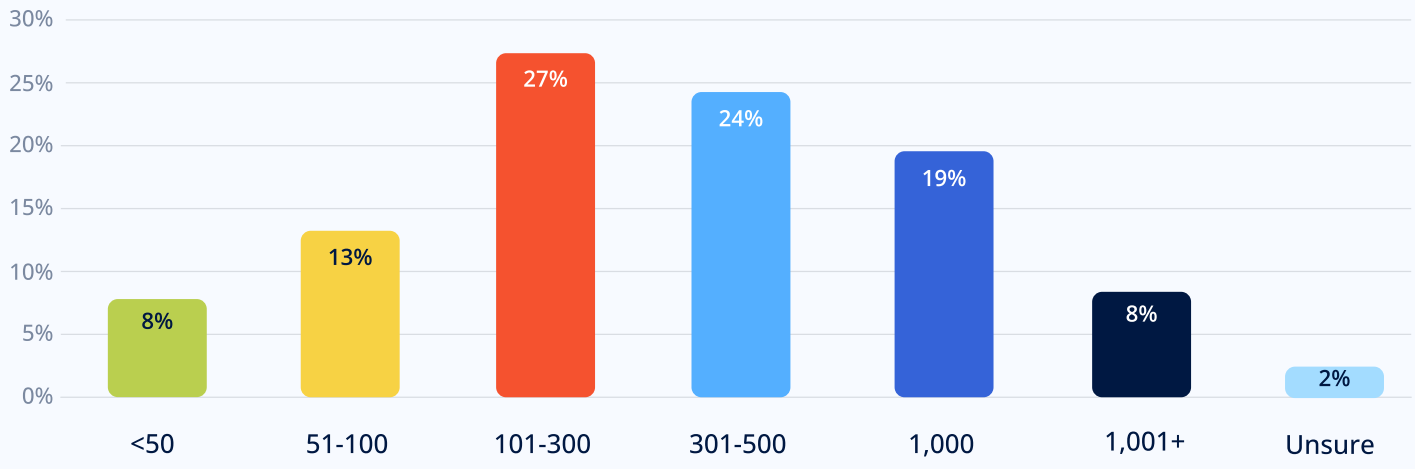
More than half of organizations (51%) oversee 300 or more vendors — including core processors, cloud and IT providers, cybersecurity firms, payment and card processors, lending and credit data services, compliance platforms, customer communication providers, and professional service firms — and some manage far more. An additional 14% have no dedicated staff at all, relying on employees who share TPRM responsibilities alongside other duties.

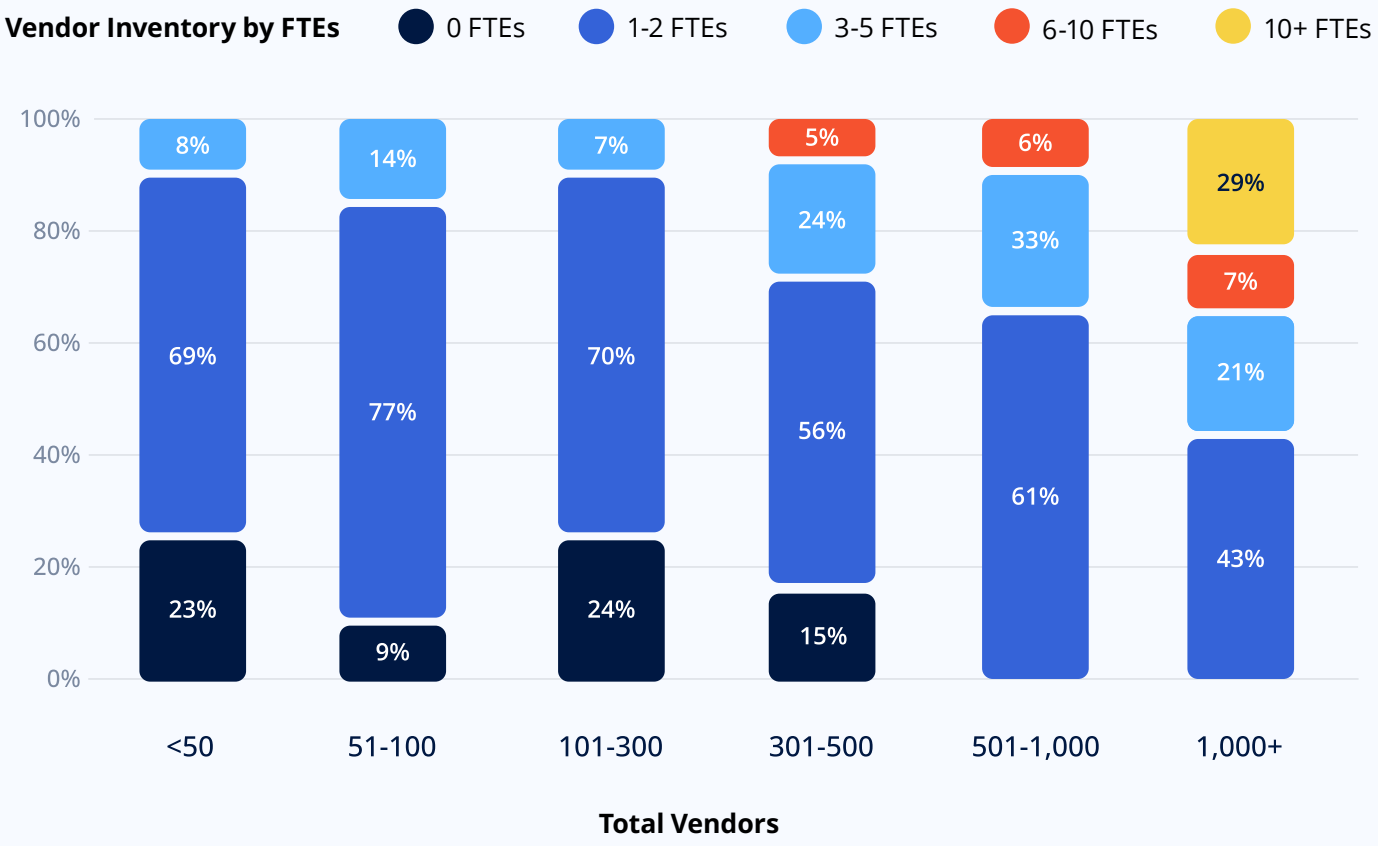


How many full-time employees are dedicated to your TPRM program?

0 FTEs (shared task) 1-2 FTEs 3-5 FTEs 6-10 FTEs 10+ FTEs

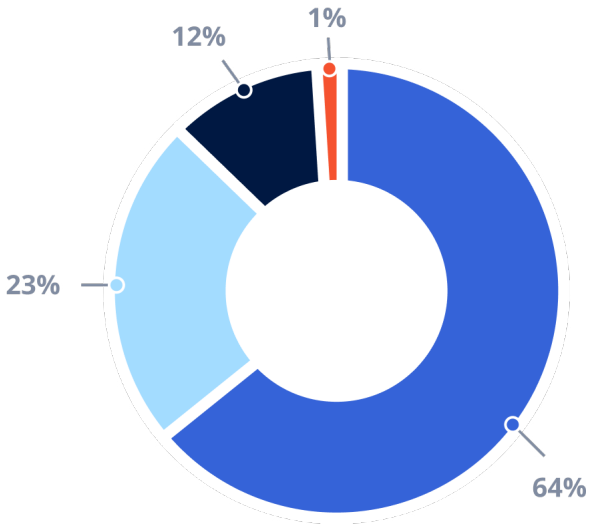
How many total vendors are included in your third-party risk management program?





That means the typical TPRM professional ends up responsible for well over 100 vendor relationships, handling everything from due diligence through ongoing monitoring and incident response, a heavy lift.

Combine this with the 64% expecting flat budgets, and you're looking at small programs tackling increasingly complex responsibilities.

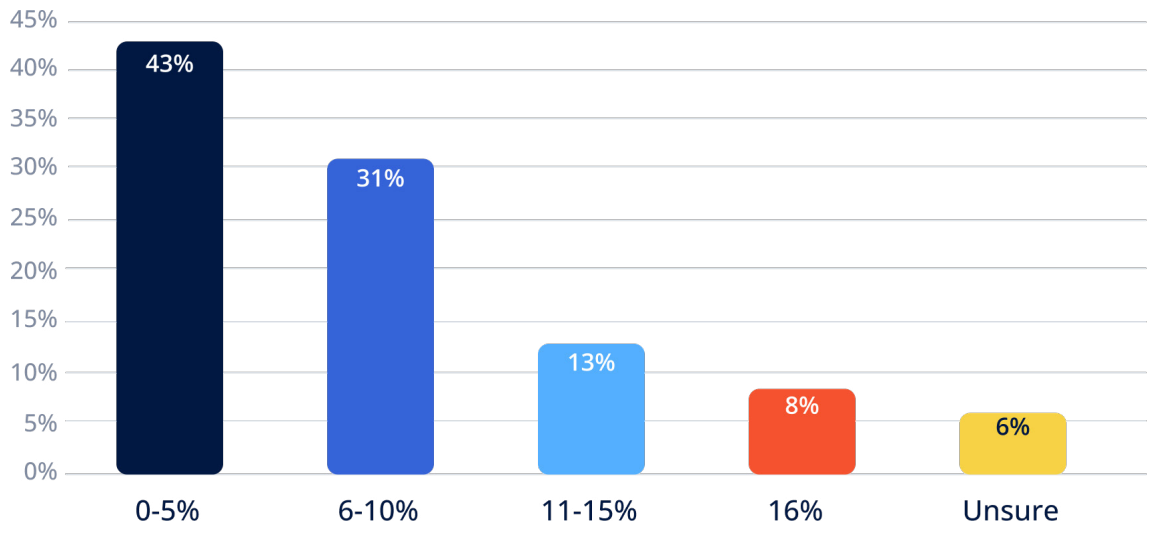


How do you expect your TPRM budget to change next year?

- Stay the same
- Increase
- Unsure
- Decrease

The good news: organizations are disciplined about criticality. Most (43%) classify only 0-5% of vendors as critical, enabling small teams to focus intensive oversight where it matters most. The challenge: even with tight definitions, a program with 300 vendors and 5% critical still means 15 high-stakes relationships requiring deep, ongoing due diligence.

What percent of your vendors are classified as critical?



Vendor Artificial Intelligence and Cybersecurity

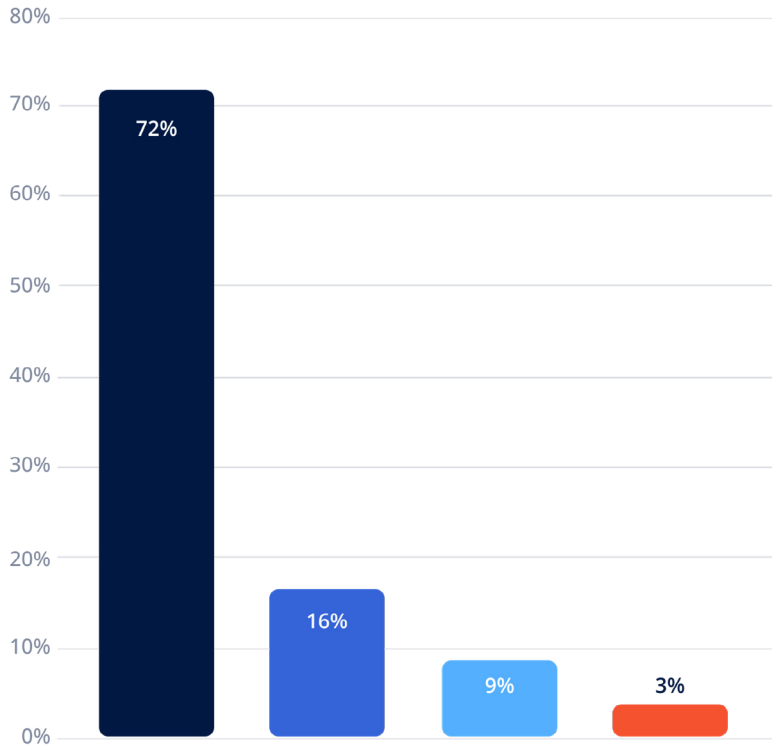
For the first time ever, artificial intelligence (AI) tied with cybersecurity as organizations' top third-party risk concern. AI is no longer an emerging curiosity, but a quickly developing risk.

Top TPRM Concerns:

1. Use of AI by vendors
1. Cybersecurity attacks at vendors
2. Vendors' operational resilience
3. Pending/anticipated regulatory changes
4. Vendors' financial health
5. Internal/systemic concentration risk

Although organizations recognize the risk, they lack the visibility and framework to manage it. Most (72%) are only partially aware of which vendors use AI, while 16% haven't assessed vendor AI usage at all. Without knowing where AI exists in their vendor ecosystem, organizations can't manage the risks or write appropriate contract language.

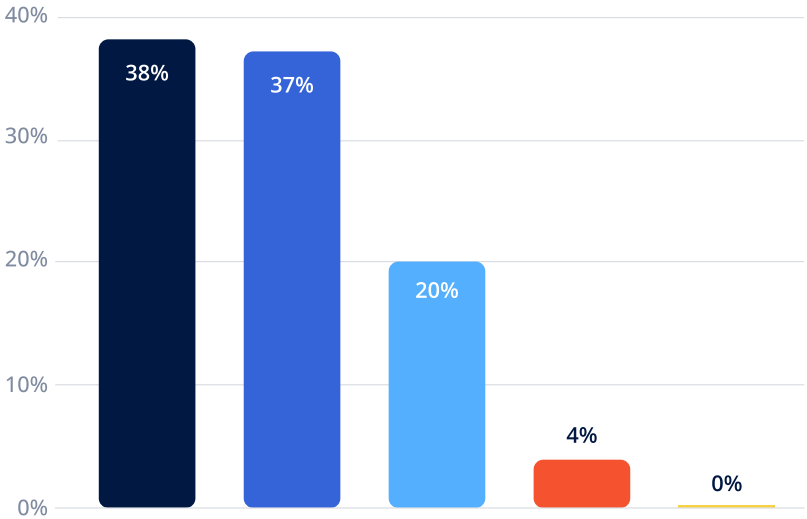
Does your organization know which of its third-party vendors use AI or machine learning within their products or services?



- Partially — We're aware of some vendors that use AI/ML, but not all.
- No — We have not yet assessed vendor AI/ML usage.
- Yes — We have identified and documented which vendors use AI/ML.
- Unsure — We don't currently ask vendors about AI/ML use.

The confidence gap is even starker. Not a single organization feels "extremely confident" managing AI-related risks. Only 4% feel "very confident," while three quarters feel either moderately (31%) or slightly confident (38%). Twenty percent aren't at all confident.

Even the most mature TPRM operations are struggling with managing vendor IT use. Just 49% feel moderately confident and 3% feel very confident.



How confident are you that your TPRM program can effectively identify and manage AI related risks today?

- Slightly Confident
- Moderately Confident
- Not At All Confident
- Very Confident
- Extremely Confident

Large Organizations Feel Least Confident

The confidence crisis is particularly acute at large organizations. Among those with 5,001+ employees, 66% feel either not at all confident or slightly confident managing AI risks — worse than small organizations (55% of those with 1-100 employees).

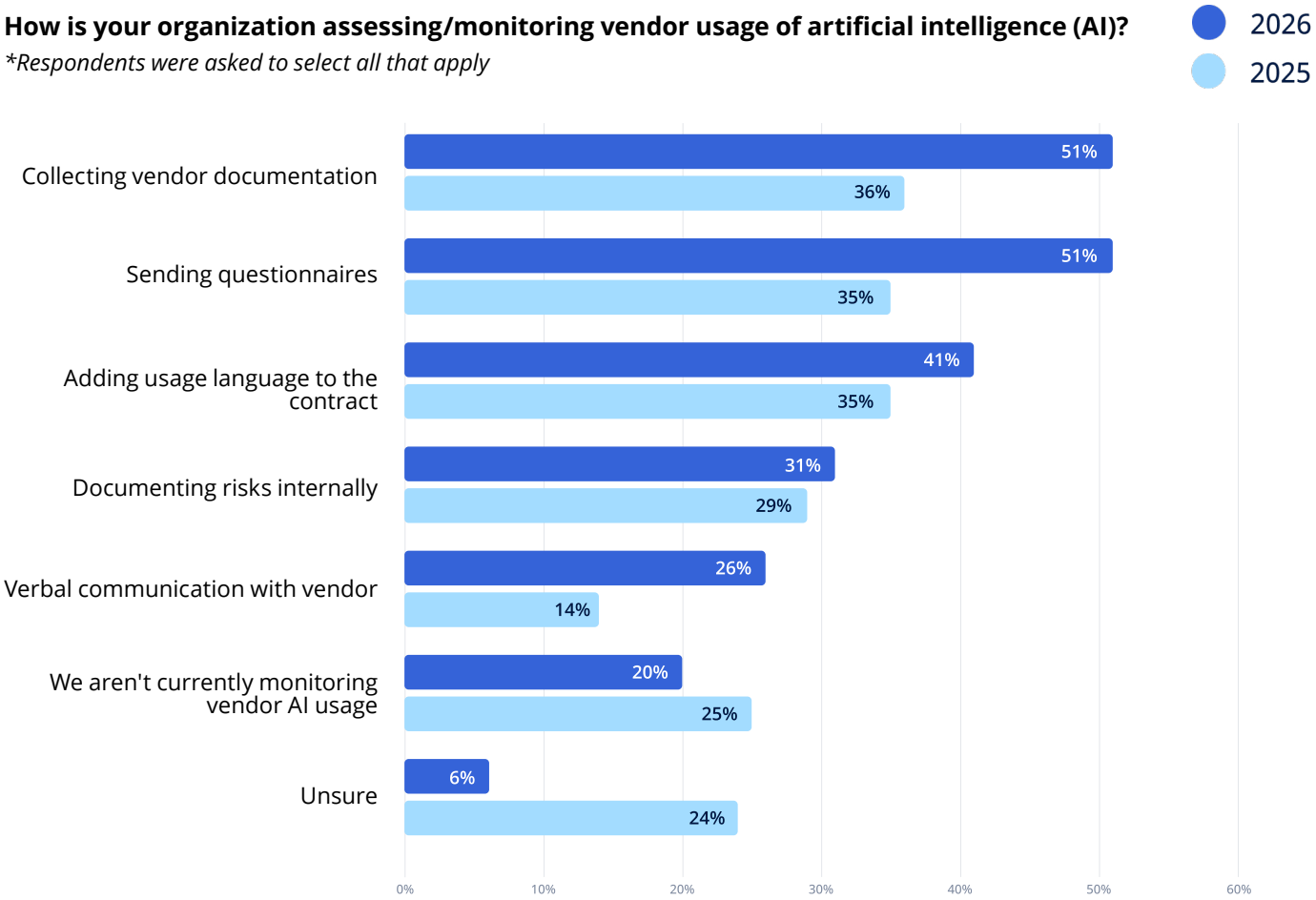
This inverted relationship suggests larger organizations either understand AI's complexity better and recognize they aren't prepared to manage that risk or they have more AI exposure across their vendor ecosystem. Either way, size doesn't translate to readiness.

AI Confidence by Organization Size

Organization Size	Not at All Confident	Slightly Confident	Moderately Confident	Very Confident
1-100 employees	35%	20%	25%	0%
101-250 employees	12%	34%	32%	5%
251-500 employees	15%	38%	33%	10%
501-1,000 employees	8%	48%	36%	4%
1,001 - 5,000 employees	23%	31%	43%	0%
5,001+ employees	33%	33%	25%	0%

How is your organization assessing/monitoring vendor usage of artificial intelligence (AI)?

**Respondents were asked to select all that apply*



Organizations Are Taking Action — But Uncertainty Remains

Despite limited confidence, organizations have increased their AI oversight efforts since last year. In 2025, 25% of organizations weren't monitoring AI usage. Today it's just 20% — steady progress, though a concerning gap remains.

The number of organizations collecting vendor documentation on AI use almost doubled, jumping from 36% to 51% — a 42% increase. As AI matures, documentation becomes more readily available to collect and organizations are starting to know what to ask for. Verbal communication with vendors about AI also saw substantial growth year-over-year (from 14% to 26%), but these casual conversations aren't going to protect organizations the way due diligence and strong contracts will.

Those unsure of whether their organization manages vendor AI risks saw dramatic declines from last year — a positive indication that survey respondents are moving toward an evidence-based approach.

Adding usage language to the contract only saw a small increase (35% to 41%). That may be due to AI contract clauses becoming more standard and less of a novelty. There was also an increase in organizations documenting the risks internally. Documentation is a critical component to ensuring compliance and demonstrating risk awareness.

Despite the positive steps forward, the lack of confidence shows organizations aren't sure if what they're doing is working and there is more work to be done.

What Keeps Organizations Up at Night

Respondents were asked to share their top three AI-related vendor concerns. Data privacy and security lead the way with other concerns not far behind.

Data privacy and security (83%): Where is the data going? Are vendors using customer information to train models?

Compliance and regulatory risk (66%): AI legislation is emerging at federal and state levels and is often conflicting or unclear. Organizations don't know what rules they'll need to comply with tomorrow, let alone whether their vendors' AI practices will violate them.

Operational risk (61%): What happens when the AI system fails? How do we maintain business continuity? Can we switch vendors if their AI becomes unreliable?

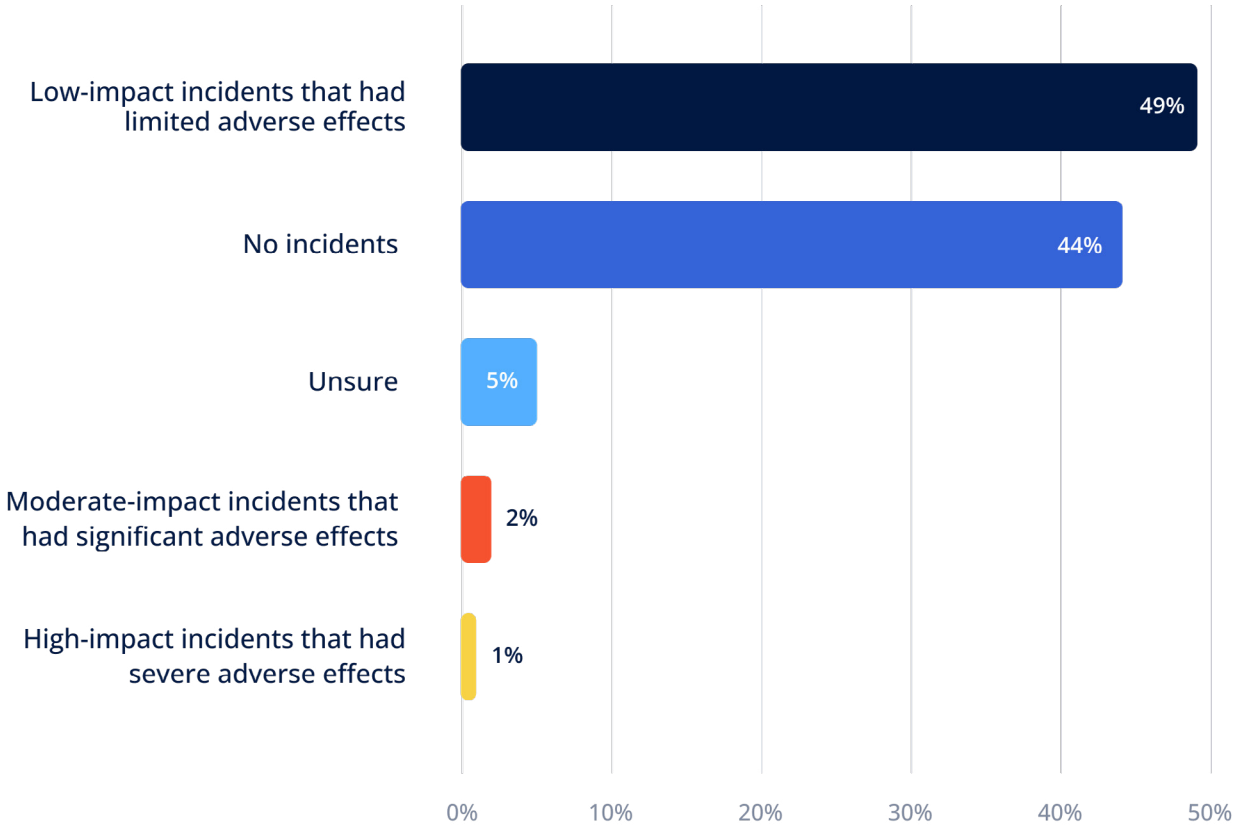
The black box problem (54%): Even vendors often can't explain their AI models' logic. For financial institutions subject to fair lending laws or required to explain credit denials, it's legal exposure.

Bias and fairness (44%): Unintentional discrimination baked into AI models creates regulatory, reputational, and ethical risks that are difficult to detect and harder to fix.

Third-Party Cybersecurity Incidents: The New Normal

Just over half of organizations (about 52%) experienced some form of third-party cyber incident. This is up from 46% in 2025. While severe incidents remain rare, the consistency year-over-year indicates that this is the new baseline.

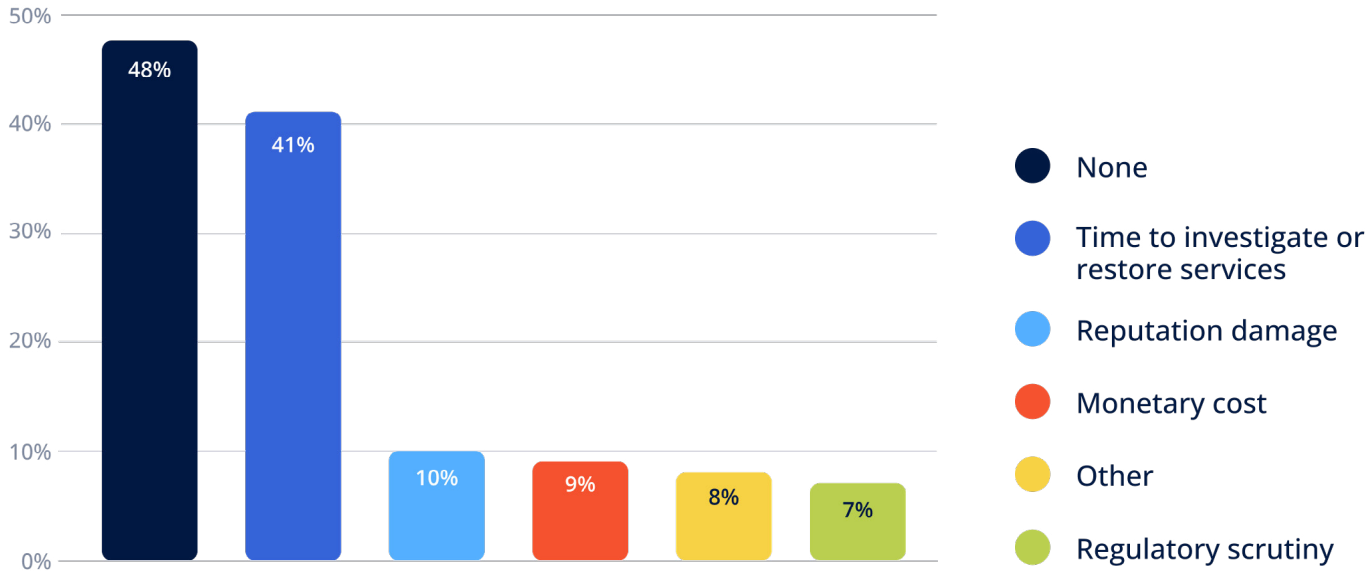
Over the past 12 months, has your organization experienced a third-party incident?



Organizations should treat vendor incidents as a recurring reality, not an exception. While 94% of the reported incidents are low impact, they are still felt. Direct financial losses and reputational damage may grab headlines, but the real strain comes from the weeks spent investigating issues, coordinating with vendors, implementing workarounds, and restoring services — all of which quietly drain productivity.

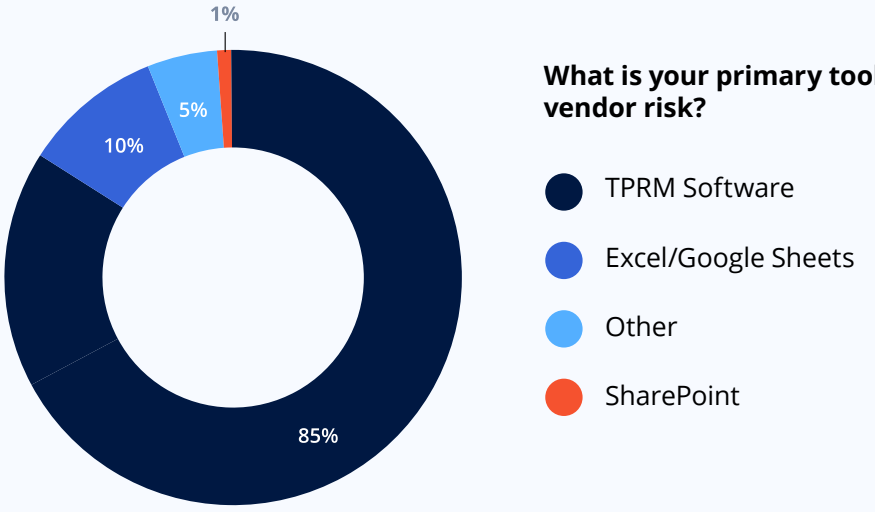
What were the biggest impacts of the incident?

**Respondents were asked to select all that apply*



Manual Processes Undermine Program Effectiveness

Dedicated TPRM platforms have moved from "nice to have" to essential infrastructure, particularly for smaller teams. Almost 87% now use either a dedicated platform or a TPRM module inside an ERM/GRC platform — up from 84% in 2025. Financial institutions continue to abandon manual processes, with just 10% still using spreadsheets — dropping from 13% in 2025.



What is your primary tool for managing vendor risk?

- TPRM Software
- Excel/Google Sheets
- Other
- SharePoint

Organizations still relying on manual processes struggle to demonstrate TPRM value and face harsher consequences during exams:

- Manual processes (Excel, spreadsheets, etc): **40% told "improvements required"**
- Software users: **28% told "improvements required"**

When it comes to exam findings, institutions with manual process users are 71% more likely to receive exam findings. When examiners can't see documented processes, consistent workflows, or audit trails, they flag deficiencies.

Those using manual processes are 50% less satisfied with their tools than those using software. Manual programs are also more than twice as likely to see TPRM as purely a compliance checkbox. When you're drowning in spreadsheets, it's hard to see strategic value.

For organizations facing cost constraints, Excel may seem like savings, but the data shows they're paying in exam findings, team frustration, and inability to demonstrate strategic value. Over half (60%) of Excel users are organizations with less than $1 billion in assets.

- **82% more likely** to get exam findings (41% vs. 23%)
- **50% lower** satisfaction
- **2x more likely** to see TPRM as pure compliance

Platform investment enables better outcomes with the same lean teams. Software users report better exam results, higher value perception, and greater satisfaction — proving that technology investment pays for itself in improved regulatory outcomes and team effectiveness.

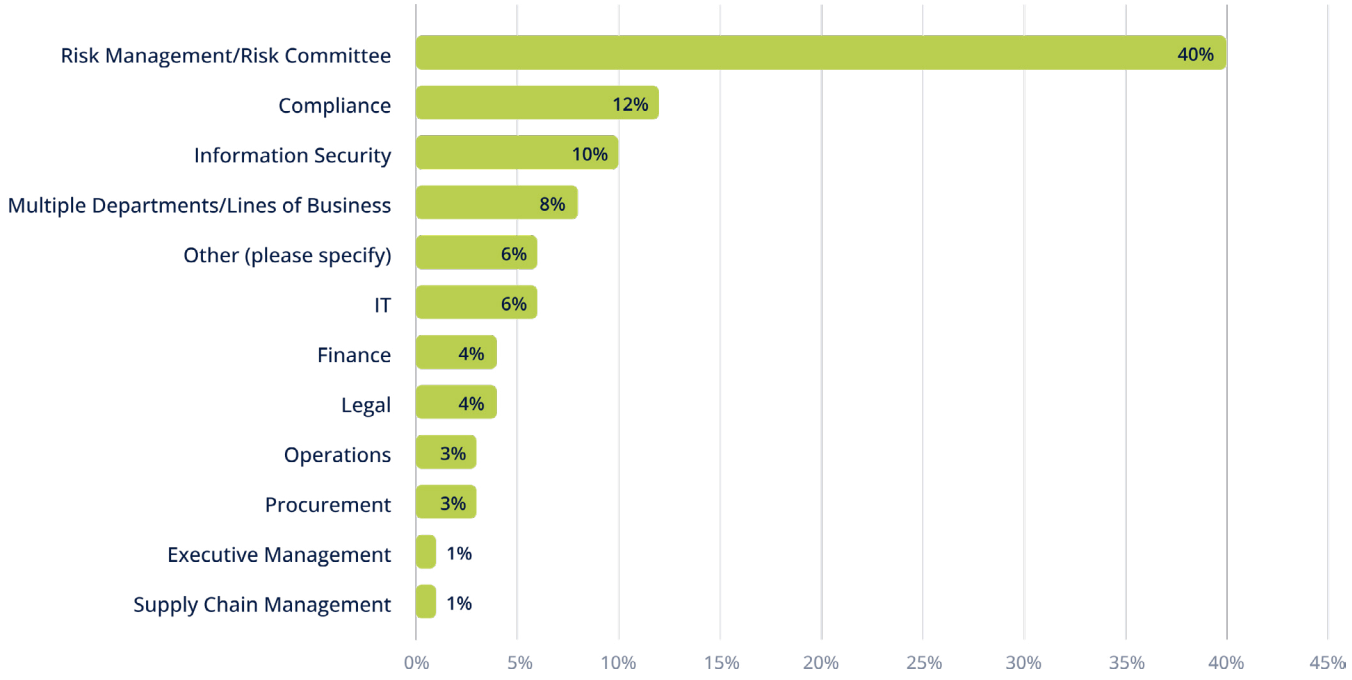
TPRM Department Ownership

Where third-party risk management sits within the organization shapes how it's perceived, governed, and enforced. Survey responses show clear patterns in how institutions structure TPRM — often reflecting their primary risk priorities and maturity.

Over half (52%) have TPRM reporting to risk management or compliance, which aligns with best practices. Putting TPRM within risk-focused departments enhances visibility, boosts credibility, and strengthens internal compliance.

The 16% reporting to information security or IT reflects organizations where cybersecurity and technology risks dominate the third-party landscape.

Which department owns TPRM activities?



TPRM Program Maturity

Third-party risk management is typically structured using one of three operating models — centralized, decentralized, or hybrid. Each reflects how responsibility for vendor oversight is shared across the organization.

Centralized model: A single TPRM team owns vendor risk management end to end, providing consistency but limiting scalability as vendor counts grow.

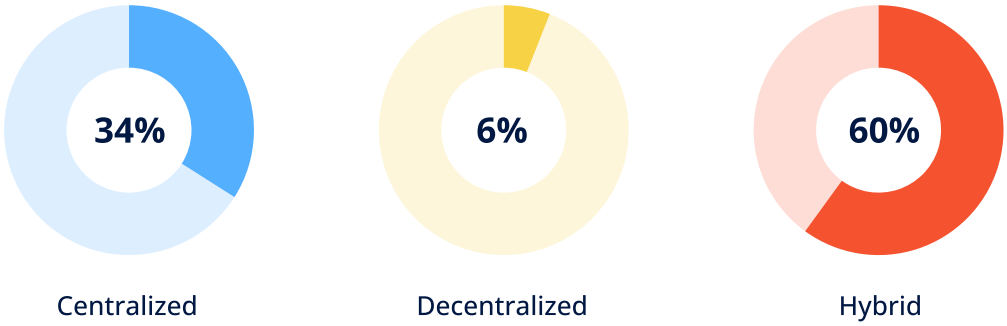
Decentralized model: Vendor owners manage risk within their business units, offering flexibility but often at the cost of consistency and control.

Hybrid model: A dedicated TPRM team sets the framework and provides oversight, while vendor owners manage day-to-day risk and performance — balancing consistency with scale.

The hybrid model continues to gain ground as the dominant approach (60% of institutions), up 15% from 2025. Among organizations using the hybrid model, 84% have established programs — having moved past ad hoc approaches into structured, documented processes. The continued popularity of the hybrid model reflects its scalability and deepening program maturity.

Centralized and decentralized models continue to decline (down 13% and 25%, respectively).

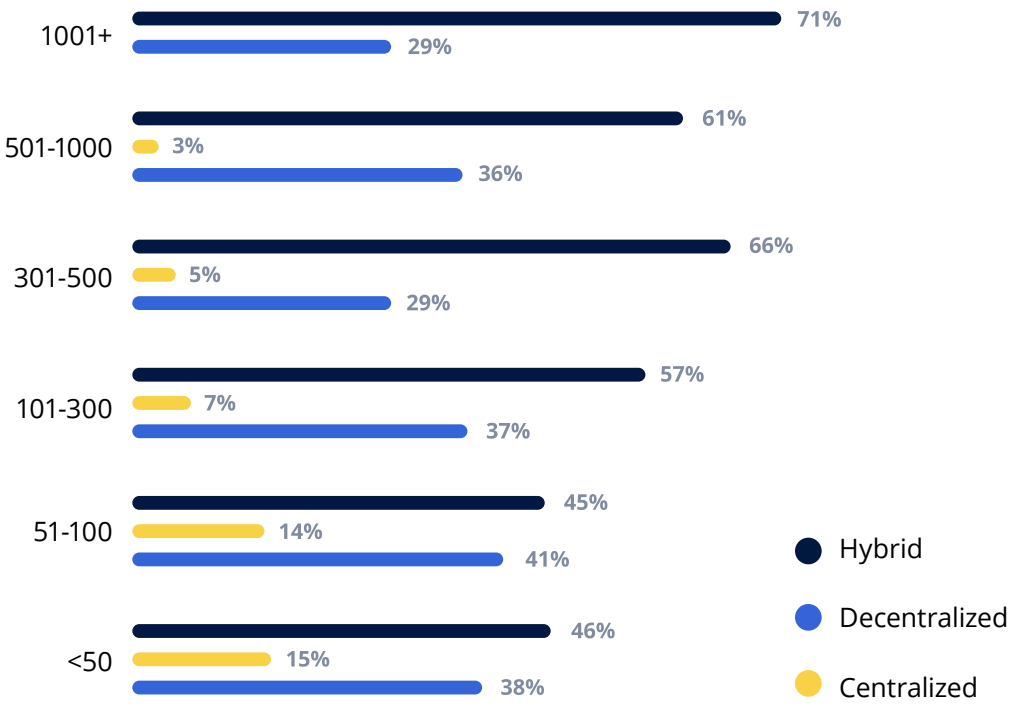
What operating model do you use for your TPRM program?



The centralized model is falling out of favor due to a lack of scalability. One TPRM team can't realistically handle day-to-day oversight of hundreds of vendors. This explains why 40% of organizations with less than 100 vendors use the centralized method. They're large enough to justify dedicated TPRM resources but small enough that one central team can still manage vendor relationships.

Decentralized models lack consistency as different business units apply different standards, which creates compliance gaps.

Vendor Inventory and Operating Models



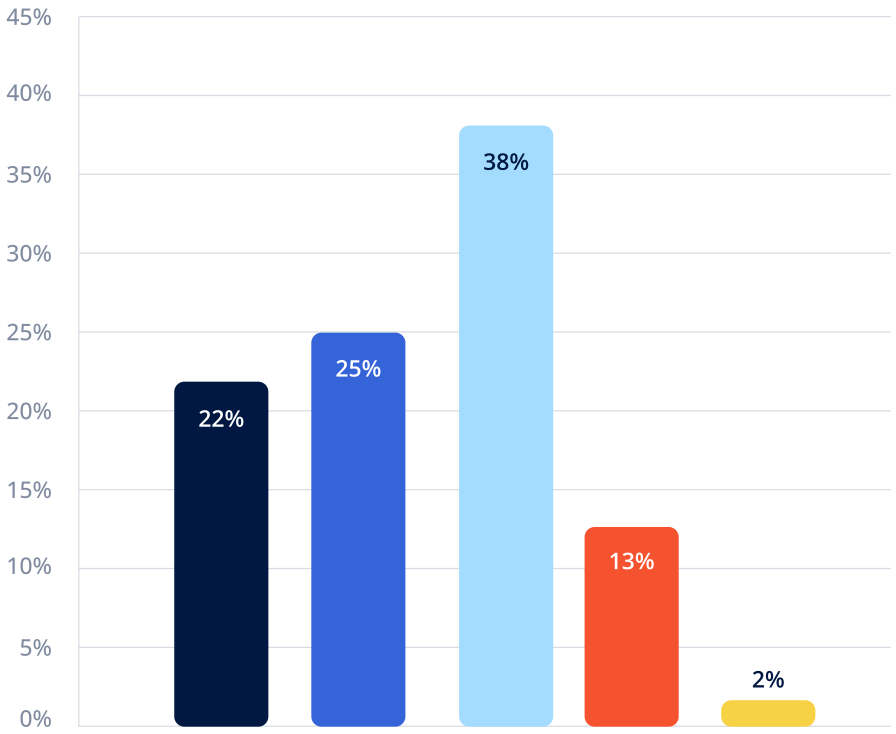
Stage of Maturity

TPRM programs range in their maturity from “Developing,” where an initial policy and program have been developed and some processes implemented, to “Optimized,” where the program is fully integrated into the overall risk management framework and continuously monitored and updated. Managed programs are fully established and integrated but don’t tie into enterprise risk management.

Over a third (38%) of TPRM programs remain stuck in “Implemented” mode. These institutions have the basics down. Policies are written, processes are documented, and tools are deployed, but they struggle to move toward value-driven TPRM.

Reaching the “Optimizing” stage (where 22% currently sit) requires executive buy-in, adequate resourcing, and sophisticated metrics.

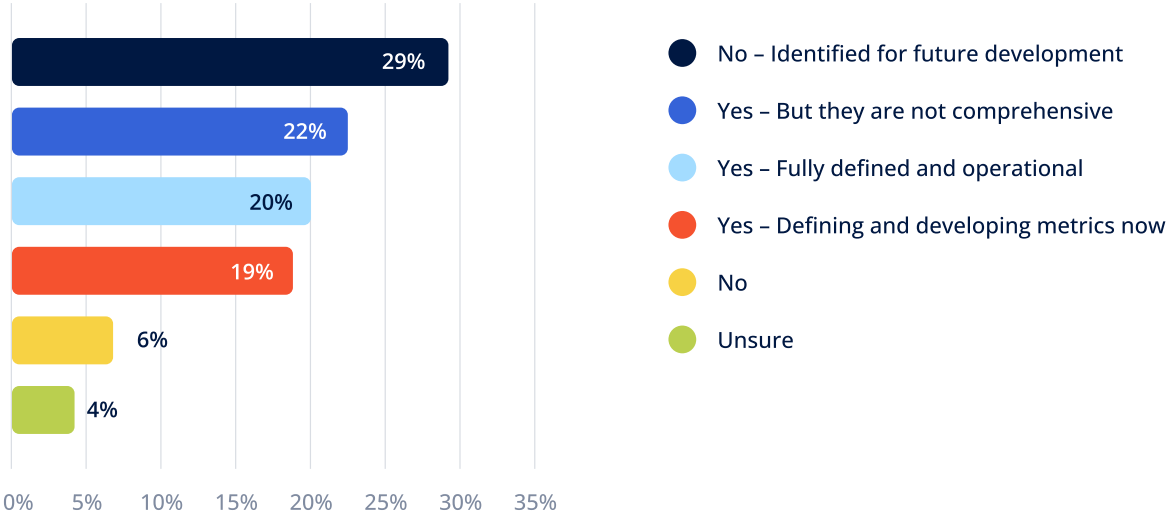
The gap between program maturity and established metrics is striking. Although organizations have implemented processes, they haven’t closed the gap with data-driven oversight.



What stage of development is your TPRM program at?

- Optimizing
- Managed
- Implemented
- Developing
- Ad Hoc

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



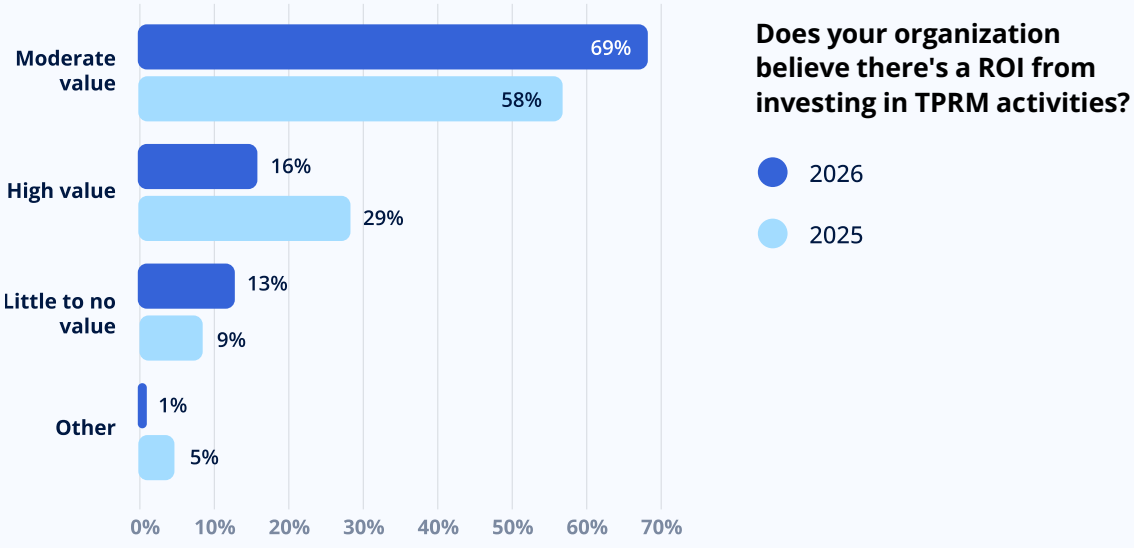
Organizational Perception of TPRM

As TPRM programs mature, organizations increasingly recognize their strategic value. Among programs at the "Optimizing" stage, 26% view TPRM as delivering high value across the organization.

At the same time, the perception of TPRM as a compliance checkbox drops sharply — from 67% at the Ad Hoc stage to just 5% at Optimizing.

This progression demonstrates that organizations investing in building sophisticated programs recognize the return on investment. They see value in cost savings from contract management, avoided incidents, operational resilience, and faster, safer vendor decisions.

The more you mature your program, the more likely you are to see TPRM as a strategic investment rather than purely compliance driven.



For decades, TPRM was simply a regulatory requirement, where most of its value was found in compliance. As vendor ecosystems — and the operational, financial, and strategic implications — grow more complex, organizations need to ensure their program aligns with their needs. Mature programs, with defined goals and metrics, clear roles and responsibilities, and dedicated technology platforms, create real value.

Maturity Level	High Value	Moderate Value	Little/No Value
Ad Hoc	0%	67%	33%
Developing	14%	68%	18%
Implemented	11%	76%	12%
Managed	18%	70%	9%
Optimizing	26%	68%	5%

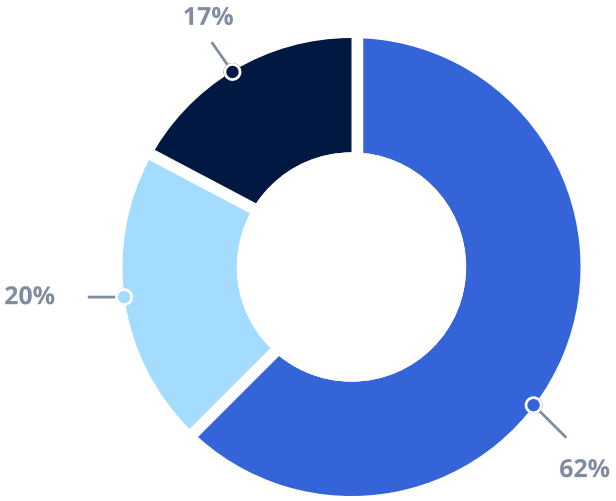
Regulatory compliance is the dominant reason survey respondents perform TPRM by a significant margin.

- **Meet regulatory requirements:** 61% ranked this as their #1 reason (Score: 5.13/6)
- **Avoid third-party cyber incidents:** 14% ranked this #1 (Score: 3.85/6)
- **Protect brand and reputation:** 11% ranked this #1 (Score: 3.64/6)
- **Align with industry best practices:** 8% ranked this #1 (Score: 3.66/6)
- **Manage vendor performance:** 3% ranked this #1 (Score: 2.36/6)
- **Control vendor costs:** 2% ranked this #1 (Score: 2.36/6)

The low scores for cost control and performance management represent missed opportunities. TPRM programs sit on a treasure trove of data, like contracts, vendor spend, performance issues, and redundancy. With proper analysis, they could drive significant operational value.

Meanwhile, institutions saying securing support for their TPRM program "isn't difficult at all" rose from 17% to 20%. That’s progress, but 79% still find it challenging or very difficult to secure support.

When TPRM teams are undervalued or viewed as compliance gatekeepers vs. risk partners, it can be challenging to drive home the strategic value.



TPRM Oversight and Challenges

Day-to-day TPRM friction continues to center on vendor due diligence and reviews. Nearly half of respondents (43%) cite obtaining timely, accurate documentation from vendors as their top challenge.

Other commonly cited challenges include:

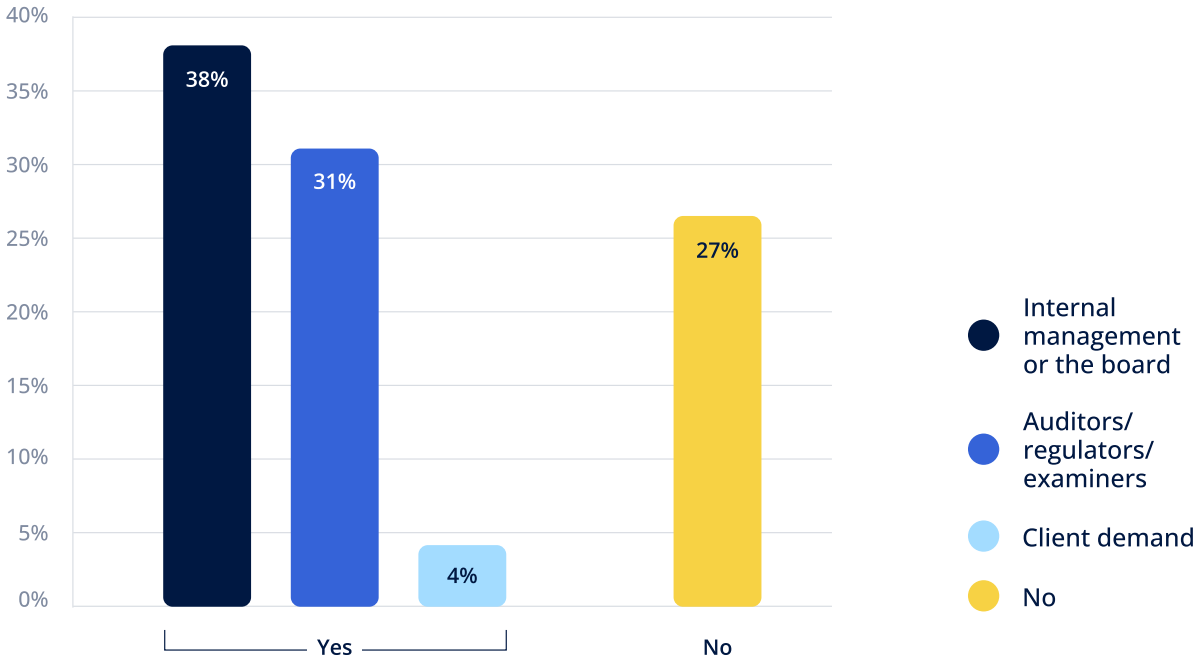
- Limited internal resources
- Difficulty automating manual processes
- Time management constraints
- Completing risk assessments

Organizations are addressing these issues through a mix of outsourcing, technology, and process improvements. Technology can’t make vendors respond faster, but it can remove much of the manual coordination that makes the process painful — automating reminders, tracking response times, and allowing vendors to upload documentation once rather than repeatedly responding to ad hoc requests.

Challenges related to internal resources and time management are closely linked. With too few people to handle growing workloads, organizations are outsourcing due diligence of critical vendors.

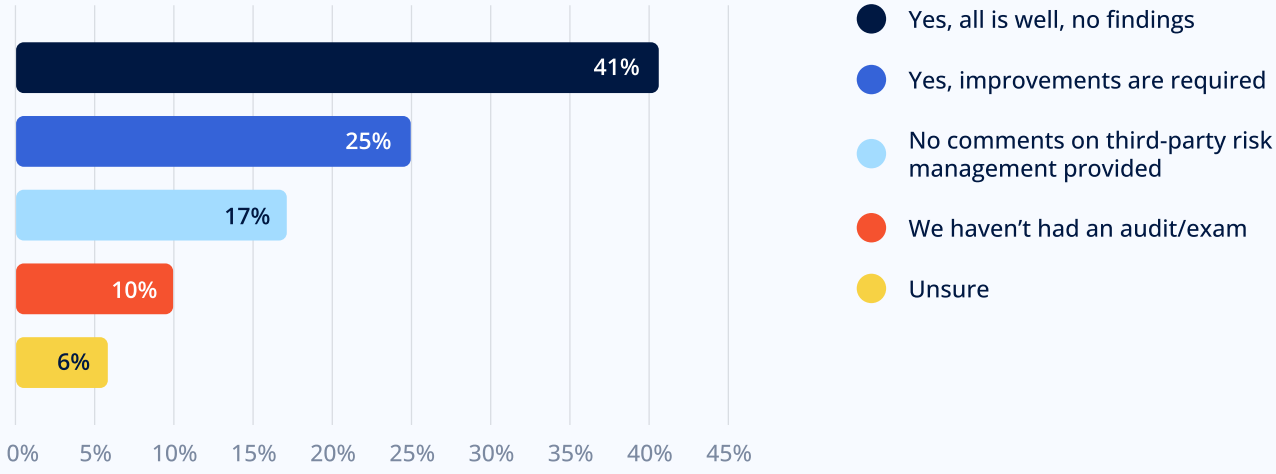
These stressors only intensify with added external pressures. Nearly three-quarters (73%) of organizations feel pressure to improve their TPRM programs. Internal management/board accounts for 38% of it, while auditors come in at 31% and client demand at 4%.

Are you feeling pressure to improve your third-party risk management program? If yes, what is the most significant source?



Boards and executives recognize that third-party failures carry consequences beyond regulatory fines. Interestingly, organizations that received no findings in their last exam or audit (37%) don't feel off the hook. More than two-thirds (69%) still report pressure from internal sources or regulatory expectations.

During your last exam/audit, did your regulator/auditors provide feedback on your current TPRM program?



Fourth-Party Risks

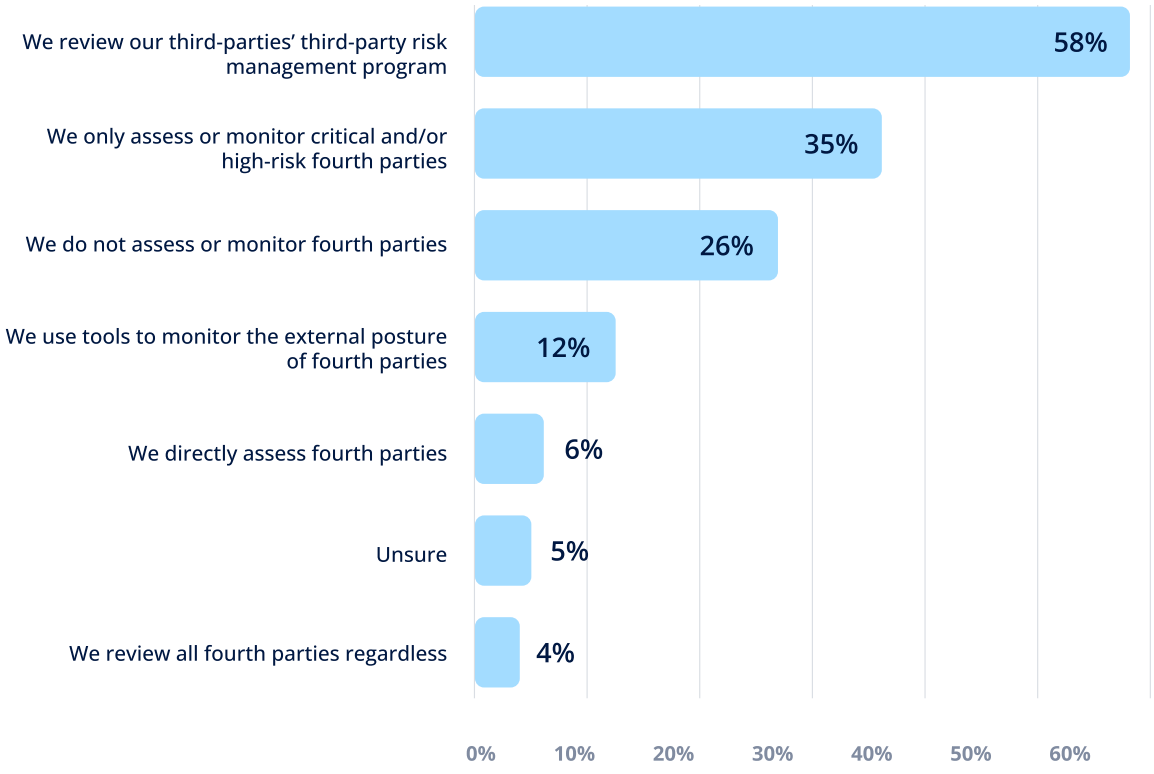
While managing fourth-party risks continues to be a challenge, many organizations have settled into a rhythm, following best practices.

Most (58%) review their vendors' TPRM programs and 35% assess their critical and high-risk fourth parties — an increase from 31% last year. Organizations recognize they lack contractual relationships and leverage with their fourth parties, so they evaluate whether their vendors are doing adequate due diligence.

A quarter (26%) don't assess fourth-party risk.

How does your organization review fourth-party vendors/subcontractors (your vendor's vendors)?

**Respondents were asked to select all that apply*



Conclusion:
From Survival Mode to Strategic Advantage

The 2026 survey reveals an industry grappling with a fundamental mismatch: TPRM responsibilities are expanding while resources remain static. With 63% of programs operating on just 1-2 FTEs, 64% facing flat budgets, and emerging risks like AI creating entirely new oversight obligations, the traditional approach to third-party risk management is unsustainable.

Yet within this challenge lies an opportunity. The organizations succeeding aren't necessarily those with the largest budgets — they're the ones making strategic choices about where to invest, what to automate, and how to demonstrate value beyond compliance.

The shift toward hybrid operating models (up 15% to 60% adoption) and away from manual processes (Excel usage down to 10%) shows the industry recognizing what scales. The 53% increase in organizations developing new metrics signals growing sophistication in measuring what matters.

But the AI confidence gap — where not a single organization feels extremely confident managing vendor AI risks — reveals we're entering uncharted territory. Mature programs where vendor management is integrated with enterprise risk management (ERM) will be in the best position to manage this new aspect of vendor oversight.

The path forward requires three fundamental shifts:

From reactive to proactive: Organizations must move beyond waiting for vendors to disclose AI usage and actively discovering where AI exists in their ecosystems — through contract reviews, technology assessments, and continuous monitoring.

From resource-constrained to resource-optimized: With flat budgets the norm, the question isn't "how do we get more staff?" but "how do we architect our programs to achieve more with what we have?" This means prioritization, intelligent automation, and strategic outsourcing.

From compliance-driven to value-creating: The data shows mature programs recognize TPRM's strategic value. The challenge is getting there efficiently. Organizations need programs that demonstrate ROI — tracking cost savings and operational efficiencies that justify continued investment.

The institutions that thrive in 2026 will be the ones that make deliberate choices about operating models, technology platforms, and risk prioritization — building programs that scale, adapt, and deliver measurable value even under resource constraints.

Recommendations and Best Practices

6 Best Practices for 2026

Make AI risk assessable, not abstract

The lack of confidence around vendor AI risk isn't surprising — most programs don't yet have the frameworks or evidence to evaluate it consistently. More mature teams are starting to build AI-specific assessment capabilities by asking sharper questions about training data, decision logic, monitoring, and bias testing, and by requesting artifacts such as model cards, impact assessments, and fairness audits. Contract language is evolving alongside these assessments, reflecting growing regulatory scrutiny and the need for clearer accountability as AI becomes embedded in vendor services.

Fix the documentation bottleneck

Documentation remains the most visible source of TPRM friction. Programs that scale are simplifying collection by narrowing requests to what's truly relevant, centralizing document libraries so vendors upload once, and offloading portions of collection where internal capacity is limited. The objective isn't faster vendors — it's fewer hours lost to manual coordination.

Right-size how work gets done

The dominance of the hybrid operating model reflects a practical response to growth. Central teams maintain standards, consistency, and oversight, while vendor owners stay accountable for day-to-day risk and performance. Supported by the right platforms, this structure preserves control without creating bottlenecks as vendor inventories expand.

Measure impact, not activity

As programs mature, metrics shift from completion counts to indicators of health and value — assessment coverage, cycle time, incidents, remediation progress, contract savings, and vendor consolidation. These measures don't need to be perfect to be useful; they create a baseline for improvement and a clearer narrative for leadership.

Optimize limited resources

With staffing and budgets largely flat, the question isn't how to do more — it's how to focus better. Risk-based prioritization, automation of repetitive tasks, and selective outsourcing allow small teams to stay focused on the vendors and risks that matter most, even as new domains like AI stretch existing capacity.

Is Your TPRM Program Keeping Up?

As vendor ecosystems grow more complex and new risks — especially AI and cyber — reshape third-party relationships, the question isn't whether TPRM needs to evolve. It's whether your program is built to keep pace. Now is the moment to step back and evaluate how risk is assessed, where effort is being spent, and whether current tools and operating models can scale with what's ahead. The institutions that act deliberately today will be better positioned to manage risk, adapt to change, and avoid being forced into reactive decisions tomorrow.

Strengthen Your Third-Party Risk Management with Ncontracts

Ncontracts is the leading provider of integrated compliance, risk management, and vendor management for the financial services industry, serving more than 5,000 financial organizations, including banks, credit unions, mortgage companies, fintech, and wealth management firms.

Focused on simplifying and strengthening all facets of risk management — including TPRM programs — Ncontracts empowers financial institutions with scalable solutions that support growth and program maturity.

Our TPRM Offerings

Nvendor
Simplify vendor management with automated due diligence, contract tracking, risk assessments, and monitoring designed for financial institutions.

TPRM Control Assessments
Comprehensive vendor due diligence providing thorough, risk-based analysis of vendor control environments.

Venminder
Manage vendors, track contract data, perform due diligence, assess risks, monitor threats, and more.

Stay Updated on Third-Party Risk Management

Webinars

Nsight Blog

TPRM Certification Training Program

Checklists, Guides & Other Free Resources

Third Party ThinkTank Community

LinkedIn