whistic

2025 Third-Party Risk Management Impact Report

Introduction
The State of Third-Party Risk Management

Each year, Whistic surveys more than 500 Information Security and Risk Management leaders to understand how the processes and approaches relating to third-party risk management (TPRM) impact the business. The result is the TPRM Impact report, a comprehensive benchmark of trends in third-party risk affecting both buyers and their vendors.

TPRM is the process of assessing, categorizing, and monitoring a complex network of third parties, so your business can make confident investments in the technology, solutions, and services you need to thrive.

And, as this year's survey findings make clear, it's never been more important.

In 2025, organizations are working with more vendors than ever before, and they're experiencing high levels of costly security breaches originating with their third parties. As a result, businesses are investing more time, money, and personnel into TPRM—but still struggling with inefficient processes, resource constraints, and costly delays in the assessment process. At the same time, the evolution of artificial intelligence has many organizations exploring a modern, AI-first approach that increases automation, agility, and efficiency.

In examining these trends, the 2025 TPRM Impact Report provides benchmarking on:

- How your peers build and execute their TPRM programs, including the resources they dedicate, the time they spend assessing vendors, and the challenges and opportunities they face.
- How your vendors respond to security assessment requests and the ways it affects their experiences, strategies, and operations.
- How both sides of the third-party ecosystem are planning for the future, modernizing, and paving the way for AI.

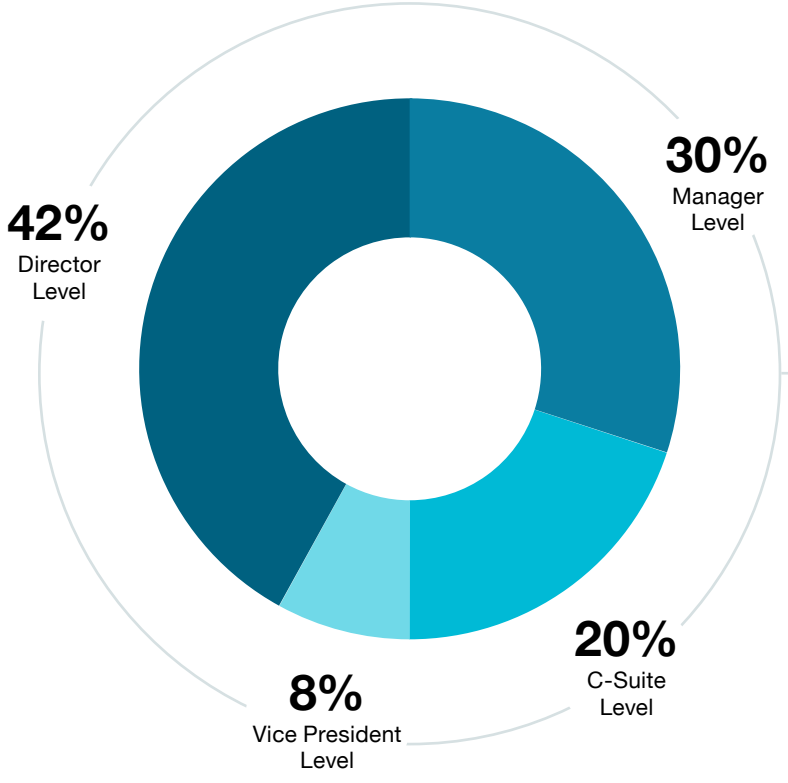
Read on for the full analysis and key findings from the 2025 Third-Party Risk Management Impact Report.

Table of Contents

Insight From the Experts
Demographics for the 2025 TPRM Impact Report

The TPRM Impact Report collects survey data from hundreds of professionals working in Information Security and Risk Management, across industries and from a representative mix of medium-to-large company sizes. Before we dive into this year's key findings, let's take a closer look at the methodology we used to build the report.

We surveyed 525 risk and information security professionals from companies with an average size of 3,100 employees. 100% of respondents serve in leadership roles and have decision-making and budgetary control over the people, processes, and technology relating to TPRM.



50%
work at companies with
500 - 2,499 employees

41%
work at companies with
2,500 - 7499 employees

9%
work at companies with
7,500 + employees

Immediate Impact

A Current Snapshot of Third-Party Risk

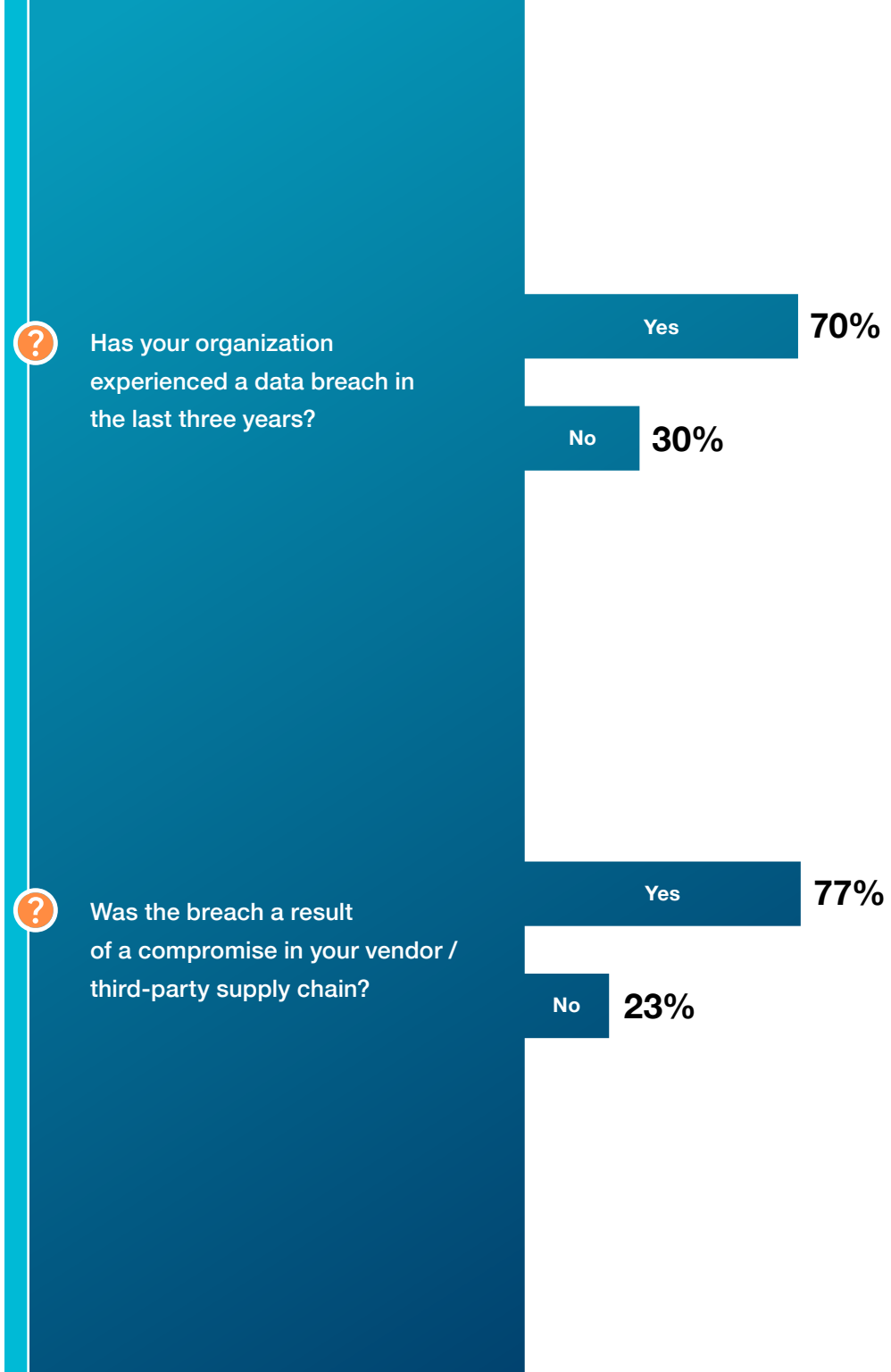
There's never been a stronger "why" for TPRM excellence than there is today.

In their annual "Cost of a Data Breach" report, IBM found that the average cost of a security breach was $4.88M per incident in 2024, which is an increase of $400K over the previous year. Whistic survey data shows that such incidents overwhelmingly start with a third-party vulnerability. And that's only the cost of an incident: failure to meet regulatory requirements around data protection cost companies like LinkedIn, Meta, and Uber hundreds of millions in GDPR violations alone last year.

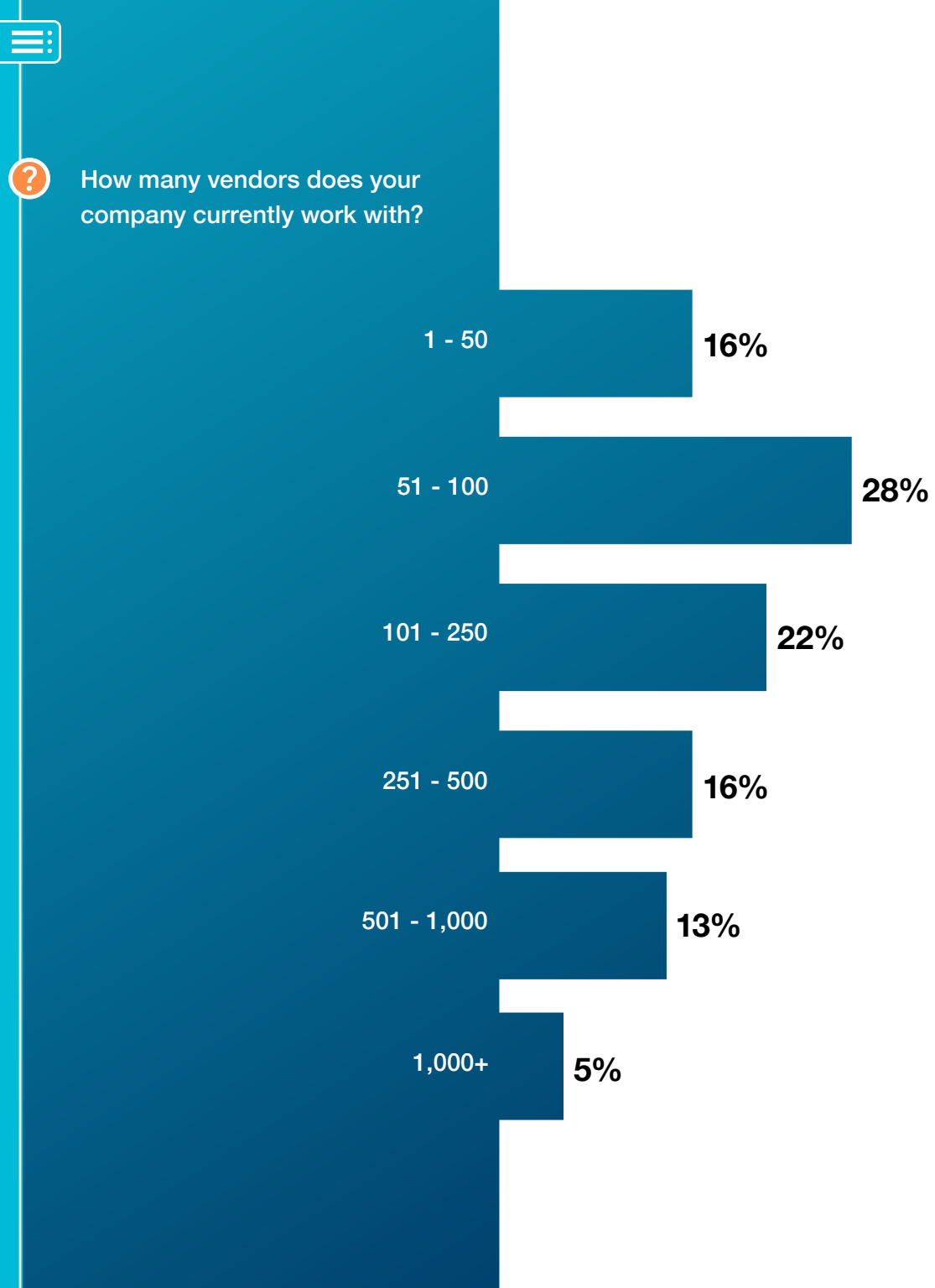
2025 TPRM trends illustrate the need for a strategic approach to risk mitigation and vendor compliance.

Key Trends

- **For a third straight year, security incidents are on the rise.** In 2023, the number of organizations that reported a security breach during a three-year period was 55%. Today, that number is 70%.
- **Third-party vulnerabilities are a major culprit in security incidents.** Over the past three years, 77% percent of those security breaches originated with a vendor or other third party.
- **Vendor ecosystems continue to grow.** In 2025, 56% of companies work with more than 100 vendors. That's a 6% increase since last year. The average number of vendors per company is now 286 (vs. 237 in 2024).



How many vendors does your company currently work with?



Key Takeaways

Increasing reliance on vendors is the inheritance of the "digital transformation" era. As medium and large sized businesses moved away from legacy technology and embraced a new digital paradigm, vendor inventories increased. There are several reasons for this:

- The increased demand for Software-as-a-Service (SaaS) offerings created new markets for developers. This specialization fueled a move away from monolithic solutions toward a growing number of narrowly focused tools.
- End users see the value in tools that are purpose-built for their needs, making them more effective and efficient than a consolidated platform that may be a jack of all trades but a master of none.
- Digital transformation increases the appetite for software-driven innovations—a trend that is now being accelerated to warp speed by cutting-edge breakthroughs in AI.

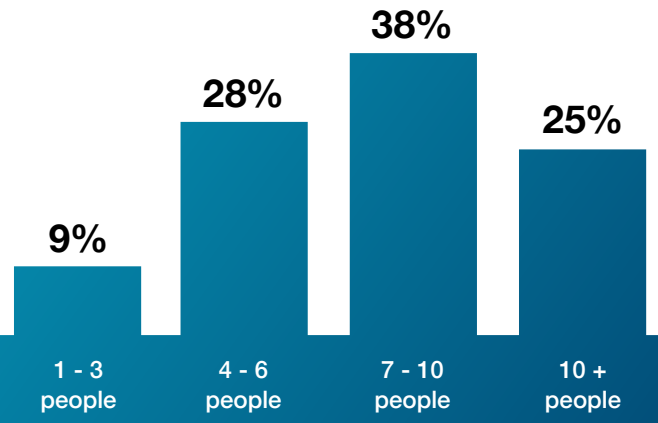
More vendors, more problems? Well, it certainly looks that way, but it's not that simple. It's true that companies use more vendors than ever and experience a very high volume of vendor-related breaches. But complexity is also increasing. This leaves businesses more exposed to third-party risk for a number of reasons:

- Diffuse ownership across the vendor ecosystem that jeopardizes a consistent approach to risk.
- Poor visibility across the vendor ecosystem due to incomplete, decentralized vendor inventories.
- High demand for services and solutions puts pressure on Procurement teams to move quickly—sometimes to the detriment of a thorough TPRM assessment.

Third-party risk management as a discipline helps organizations to face these challenges. In the next section, we'll take a look at how companies are executing their TPRM strategies in 2025.

The "Who" and 'How" of TPRM in 2025

The full impact of TPRM goes beyond simply meeting a compliance requirement and whether or not a third-party vulnerability becomes a breach. The strategic and tactical decisions companies make about building, leading, and supporting a vendor risk program can have huge effects on business outcomes. Here's a look at how organizations are approaching that task in 2025.



What is the size of the team in your organization involved in conducting vendor assessments?

Key Trends

- **TPRM teams are growing.** The size of the average TPRM team has grown in the last year to 8.5 individuals (compared with 5.6 in 2024)—though 75% of companies still have a lean TPRM team of fewer than 10.
- **…and so is the cost.** The average cost to hire for your TPRM team this year is nearly $116K annually, an increase of $6K over last year. 80% of respondents intend to add headcount this year.
- **Additional resources are desperately needed.** With an average vendor inventory of 286 third-parties and an average TPRM team of 8.5, the average vendor risk professional is responsible for assessing 33.6 vendors. This does not include vendors that are procured throughout the year.
- **The vendor experience is paramount.** 99% of respondents say that vendor experience is at least somewhat important during the assessment and onboarding process—and 70% say it is critically important.
- **Assessment teams are looking to augment the traditional security questionnaire.** The move away from a questionnaire-only approach to vendor assessments is slowly taking place, while an appetite for supplementary data sources is increasing:
  - 75% of companies are using a customized questionnaire for their assessments, which is down from 79% in 2024.
  - 83% of companies now use some kind of exchange—a centralized repository for on-demand vendor security documentation—as part of their assessment process.
  - 88% of companies leverage security risk ratings in their process.
  - 74% of companies accept a previously completed standard (like SIG, ISO, or CAIQ) in lieu of their typical questionnaire, while 93% of companies will at least begin an assessment with a previously completed standard.

Key Takeaways

- **TPRM teams struggle to keep up with demand.** Even as teams grew in the last year, companies still see the need to increase their investment in TPRM resources. That's because the gains in headcount struggle to keep pace with the increase in vendors.
- **The questionnaire has become a chokepoint in the process.** With such high demand, a single source of vendor intelligence is simply not effective for doing a proper assessment. We'll discuss the time that goes into vendor assessments in the next section, but it's clear that buyers are seeking other data sources to increase the flow of information.
- **Better vendor experience, better assessments?** Companies are betting that if they can make the assessment process more streamlined for their vendors, they will improve TPRM outcomes. When the burden of the assessment is eased, vendors are much more likely to respond fast to assessment requests and become more engaged partners during the process.

Want to Learn More?

Building and nurturing a strong TPRM program takes a disciplined approach. Check out these additional resources as you benchmark and evolve your approach:

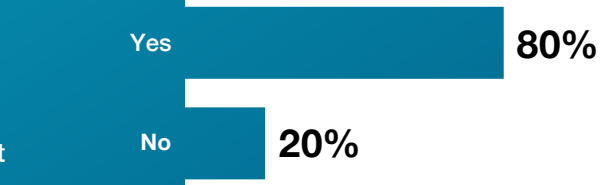
Where does your approach stack up to industry best-practices?
Find out with our free TPRM Maturity Quiz

Take the Quiz

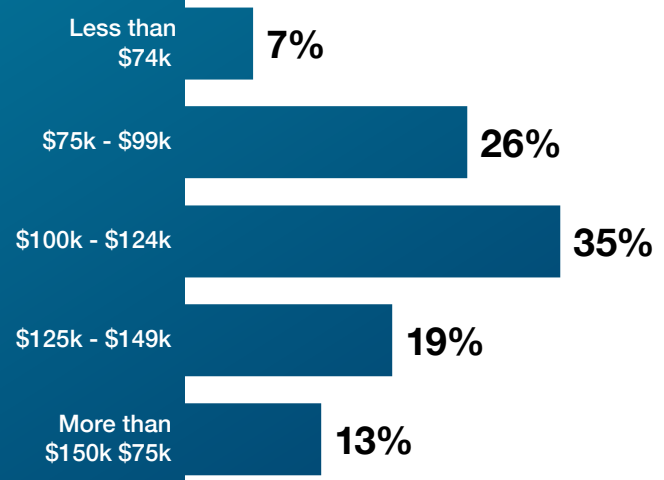
Now that you have a baseline for your program, get ready to take the next leap forward with the Total TPRM Maturity Checklist.

Get your Copy

Do you plan to hire someone to assist you in conducting vendor assessments in the next 12 months?



What is the average annual compensation (salary, bonus, and benefit costs) for the individuals performing the bulk of the vendor assessments at your company?



Conducting Vendor Security Assessments
Impact on Buyers and Customers

TPRM outcomes—reduced risk, compliance, customer confidence—are important indicators of a healthy program. But they only tell part of the story when it comes to true impact. That's because every company has unique regulatory requirements and its own risk appetite. These factors can change over time (or very quickly), making it hard to measure the overall effectiveness of your program based on outcomes alone. After all, you can't measure the breach that didn't happen, or evaluate your approach to compliance when past regulations no longer apply.

The holistic impact of your TPRM process is felt in terms of the time and resources necessary to hit established benchmarks tied to the vendor assessment process. These include:

- **Number of vendors to assess.** This number is based on the inherent risk of the vendor, the types and volumes of data they can access, and their criticality to your business. Respondents to our survey will assess an average of 255 vendors this year.
- **Assessment cadence**. How often is it necessary or prudent to reassess each vendor based on established risk factors?
- **Business demand for vendor products and services.** This can fluctuate based on a number of factors—an emerging market, a new product line, competitor behaviors, new innovations, or opportunities for cost controls. Your TPRM approach should be able to scale with demand to deliver necessary solutions quickly and efficiently.

When combined with high-level outcomes, your capacity to meet these objectives paints a more vivid picture of your TPRM program. In this section, we'll look closely at the vendor assessment process and its demands on time, resources, and costs.

Bang for the Buck

Cost vs. Benefit in Vendor Risk Management

2025 survey data suggests that many organizations are struggling to match the overall costs of TPRM (in terms of dollars, time, resources, risk levels, and opportunity cost) to commensurate value. Here's the story that emerges, by the numbers:

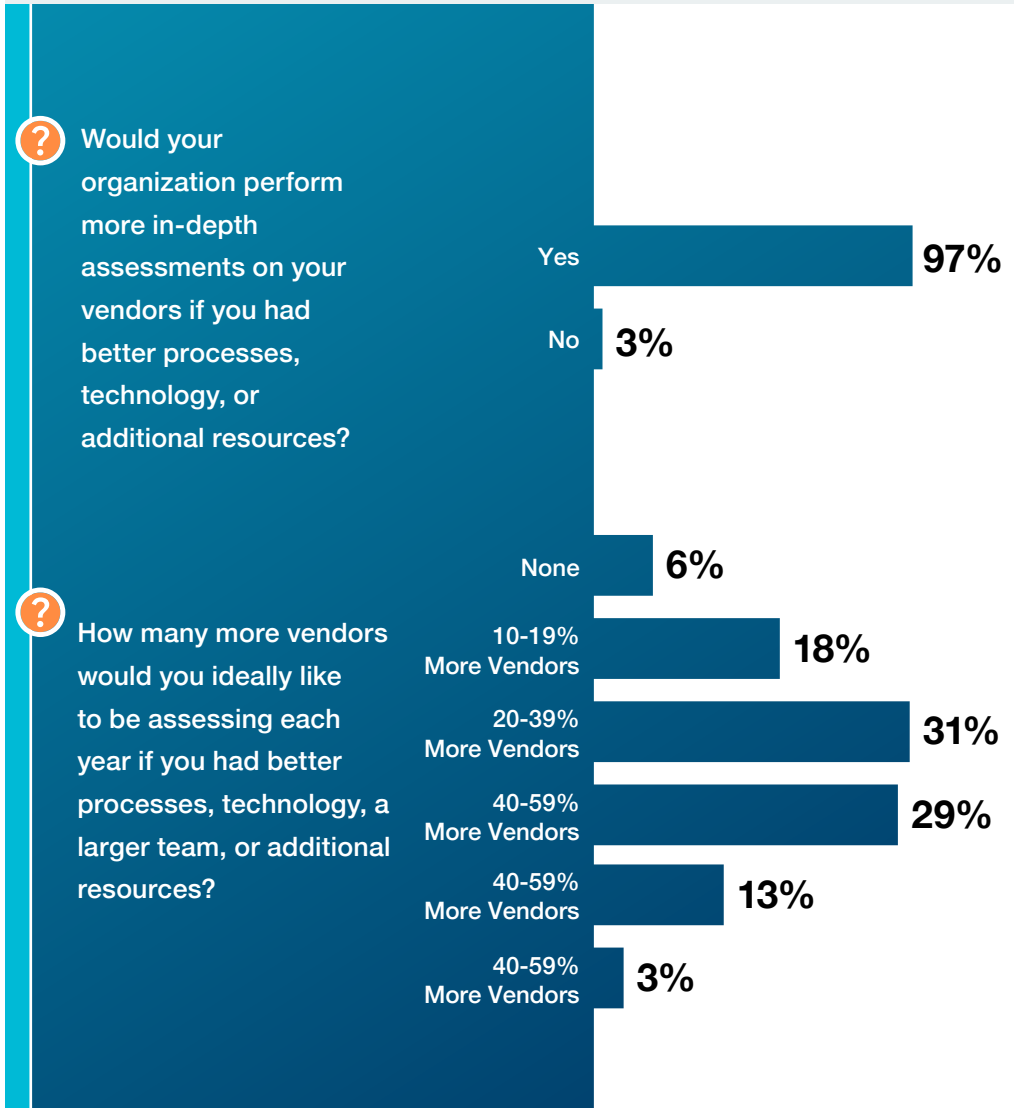
- Over the last year, the average company added roughly 3 people to its TPRM team (growing from 5.6 persons to 8.5). In 2024, the cost of adding one person was $109K, for a total investment of ~$320K.
- 80% of companies report a desire to increase team size again, at an average cost of $115K per hire.
- In spite of these additional investments, 94% of companies report they would assess more vendors if they had more time, resources, and technology—which means vendors that should be assessed by these companies based on their own risk criteria are not being assessed. In short, these companies are taking on more risk than they would like.
- Additionally, 97% of companies surveyed report they would do a more in-depth and detailed assessment if they had greater capacity—again, leaving risk management to chance.

Growing vendor inventories are accelerating third-party risk, and the investments in talent intended to stem the tide are simply not keeping pace. To understand why, let's take a closer look at the burden of the assessment process and the strain it places on resources.

Want to Learn More?

If you're interested in improving the ROI of your TPRM program, check out this executive-level, on-demand webinar.

Watch Now



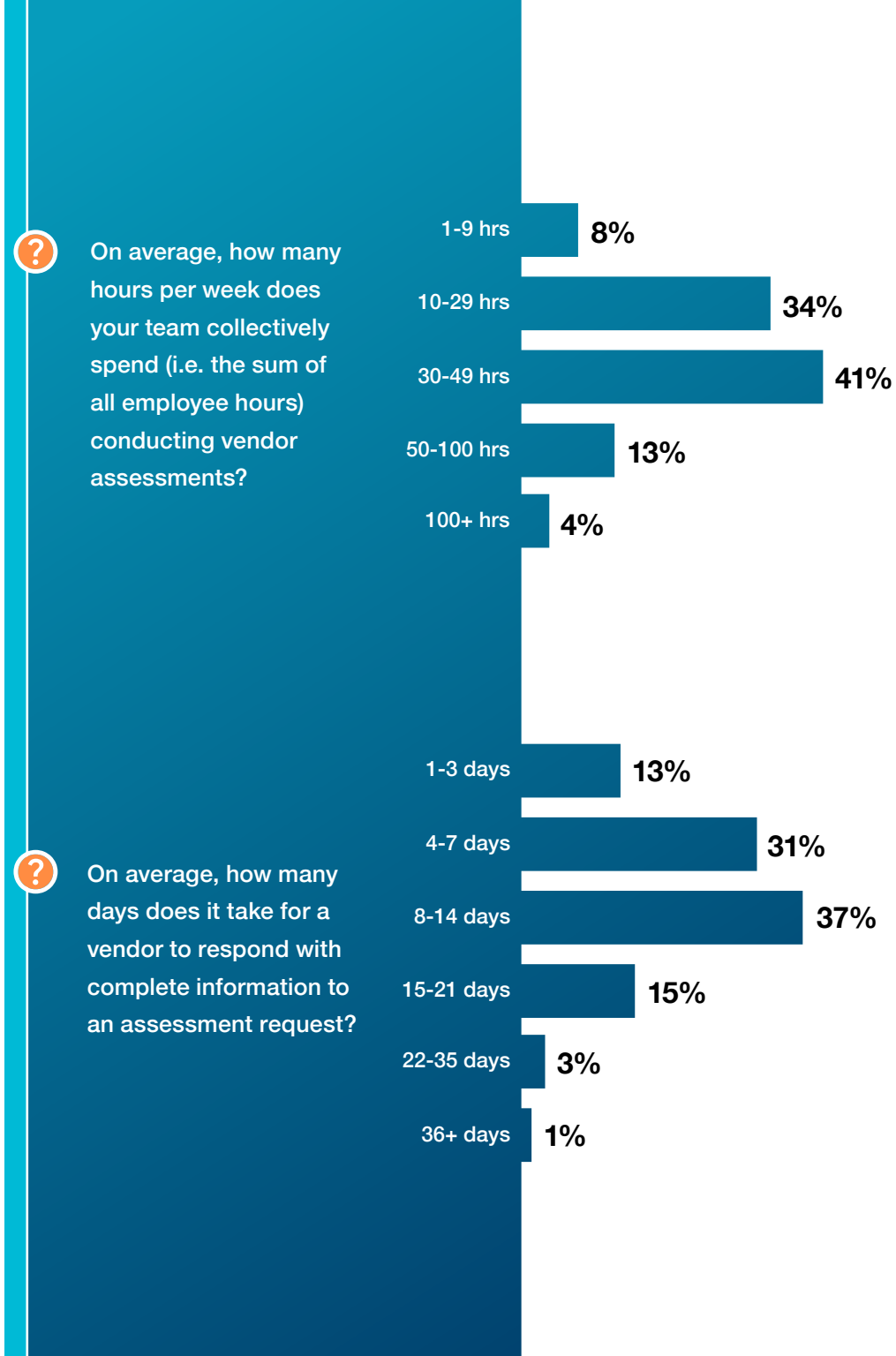
Time Keeps on Slipping

Understanding the Impact of Vendor Assessments

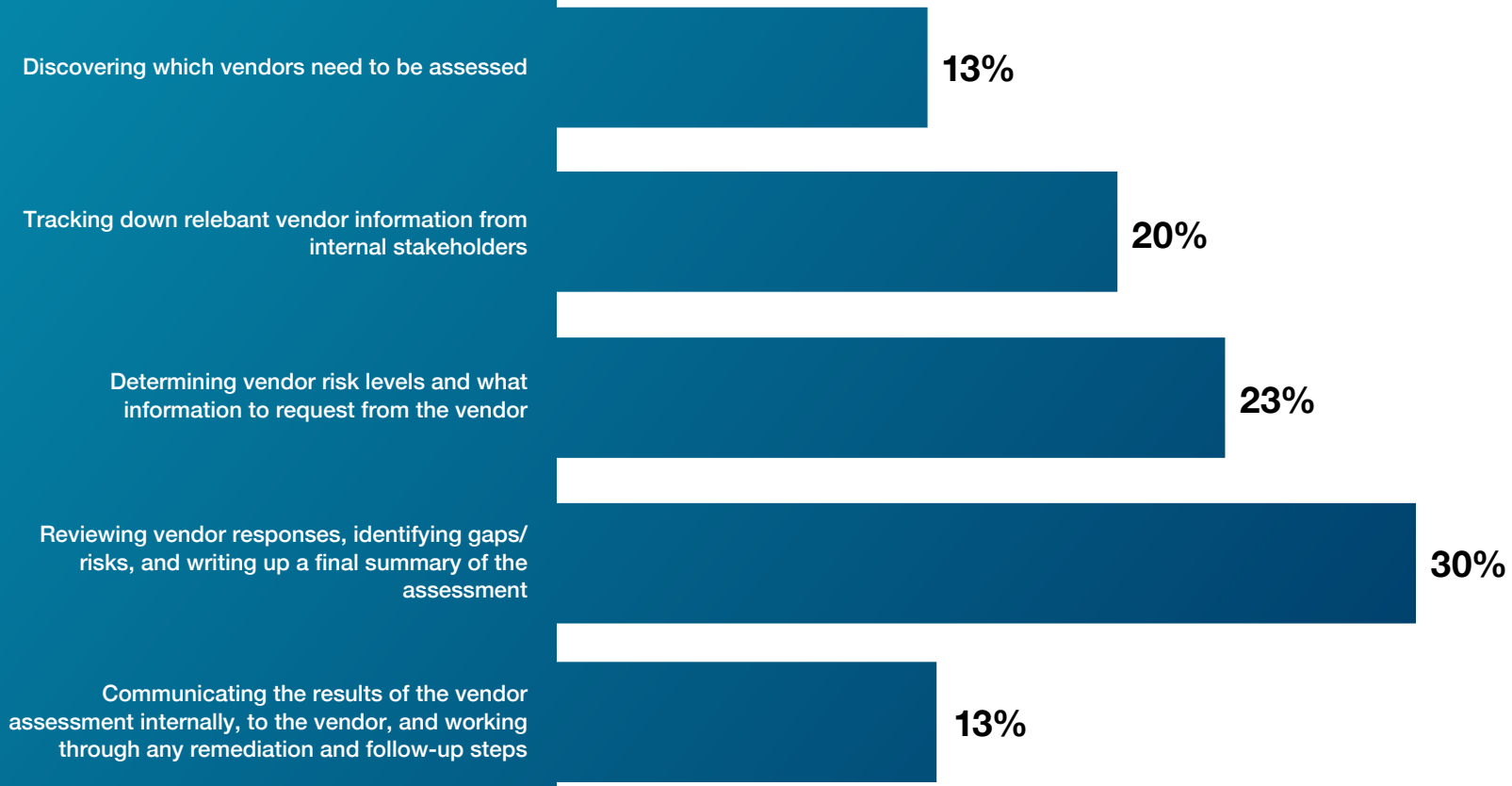
Time is perhaps the most important variable in understanding the high-cost impact of TPRM in 2025. Here are some of the time demands (and constraints) facing teams this year.

Key Trends

- **Assessments are taking more time, not less.** 58% of companies spend more than 30 hours every week conducting vendor assessments; that's a 25% increase over last year. The overall average is 37.4 hours (up almost 14 hours per week since last year).
- **Waiting with bated breath.** Response times from vendors are also getting longer, adding days or weeks to the process. 87% of companies wait longer than 4 days to receive a response from a vendor (an increase of 13% from 2024); 56% of companies wait more than a week (that's 20% longer than last year); and data shows that the average vendor response time is actually about 12 days.
- **It's never right the first time.** 84% of initial assessments require some kind of follow-up action from the vendor. Fingers crossed you're not waiting an extra 12 days!
- **The time burden has shifted to the assessment team.** 88% of companies either almost always or always have to sift through vendor documentation themselves for a specific control gap, data point, or piece of evidence.
- **Common risk mitigation adds time.** The average company surveyed experiences 7 annual security incidents (like last year's Crowdstrike event or other Common Vulnerability and Exposure) that trigger a vendor outreach; that's up from an average of 4 such incidents last year. Companies spend an additional 14.8 hours per incident on reassessments and vendor follow-ups. Over the course of year, that's more than 100 hours; what could your team accomplish with an extra 100 hours each year?



When conducting a vendor assessment, which part of the assessment takes the most time?



Responding to Assessment Requests
Impact on Vendors and Customer Trust

99% of companies say that the vendor experience during a TPRM assessment is important to them. Yet vendors and third parties still feel the burdens of time and complexity—along with the pressure to respond to a seemingly endless list of assessment requests from customers and prospects. They feel the impact in a number of ways, including:

- **Security documentation bottlenecks.** The documentation necessary to respond to an assessment request remains decentralized in many organizations—it may live in several repositories, spreadsheets, audit reports, or trust centers. It's also often controlled by InfoSec, making them the only source of truth for the organization.
- **Sales teams are diverted by requests.** Out of necessity, Sales often plays a role in questionnaire-based assessments. This delays closed deals and takes time away from selling.
- **Proliferation of TPRM tools.** 93% of companies conduct their vendor assessments with some kind of technology platform. While in some cases this can increase opportunities for automation, it also means that vendors must manage requests, communication, and licenses for dozens of different systems to accomplish the same task.
- **Manual tasks still factor heavily.** As we mentioned in the previous section, the average vendor takes 12 days to respond to an assessment request. While vendors face many of the same resource and technology constraints as their TPRM counterparts on the buyer side, the manual process of responding to questionnaires and attending to follow up is still a massive factor. Manual steps cause delays and increase the likelihood of errors that prolong the back-and-forth.

In this section, we'll take a look at the factors that contribute to these challenges for Customer Trust teams.

Striking a Balance

Time, Resources, and Expectations in Customer Trust Programs

Security is every bit as important to vendors as it is to their customers. After all, their bottom line depends on developing secure products built on a foundation of consumer trust. They also face the same cybersecurity threats and third-party risks their own customers face, so they understand the impact of TPRM.

But because no customer's risk tolerance or regulatory pressures are the same, vendors face a wide range of assessment types. Here are some of the ways this complexity and variance impact the assessment response process.

Key Trends

- **Surprise, surprise…assessment requests are on the rise.** If you've come this far, you won't be shocked to learn that 51% of vendors respond to 25 or more assessment requests every month—that's 11% more vendors in this bracket compared with 2024. In fact, the average vendor now responds to 37.3 assessment requests every month. That's up from 29.5/month last year.
- **Assessments are completed piecemeal.** On average, a complete assessment response takes 4.8 hours per request. That's no small feat, but the work is rarely done in a concentrated timeframe and in fact usually takes place over a period of days or weeks.
- **The hours add up.** Given the average time it takes per response and the average number of responses in a month, the typical vendor spends 179 hours every month on completing assessments—that's the equivalent of someone spending every hour of every work day in a month on assessment responses...and still having 20 hours of work left over.

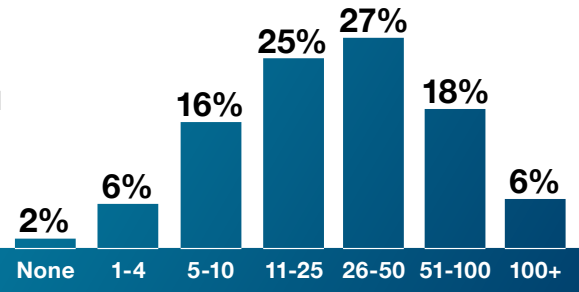
Want to Learn More?

If you're looking to build trust faster and ease the burden of assessment requests, **check out these 5 pro tips for building a great trust center.**

Learn More

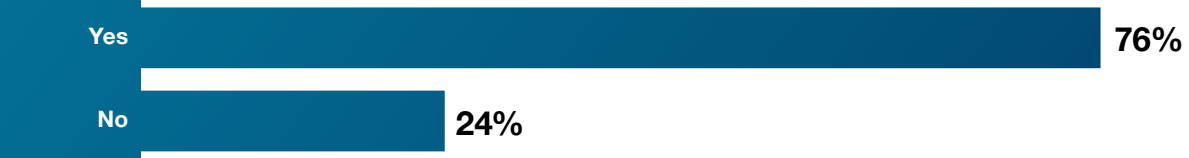
- **Proactive transparency eases the burden on response teams.** 76% of vendors make security documentation available to customers via a trust center, and it makes a difference—100% of companies surveyed deflected some percentage of incoming requests this way.
- **Questionnaire fatigue is real.** In addition to sharing a trust center to deflect questionnaires, roughly 33% of vendors will either share raw documentation like a SOC 2 audit report or previously completed questionnaire OR simply not respond in hopes of avoiding this step in the sales process.

On average, how many security questionnaires does your team respond to in a given month?

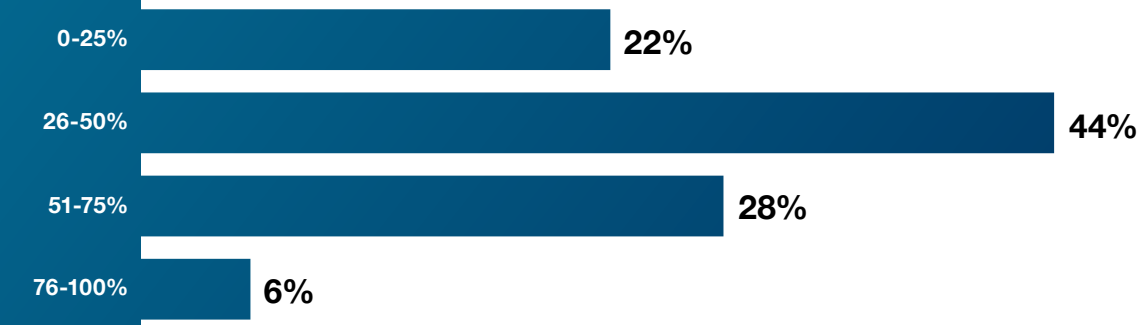


On average, how hours does your team spend on each security questionnaire response?

Do you currently make your security documentation available publicly to customers and prospects via a trust center?



On average, what % of security questionnaires are deflected when you proactively publish or share your documentation before you receive a request from your customer?



Moving Toward Modernization
The AI Present and Future of TPRM

As we've seen, TPRM teams in 2025 still struggle to balance rising demand for vendor solutions with the need to mitigate cybersecurity vulnerabilities, meet regulatory requirements, and overcome resource constraints. Companies are spending more money and time on TPRM, but they're still failing to thoroughly assess the volume of risky vendors necessary to actually mitigate risk.

This is a consequence of "legacy" TPRM. In the legacy approach, finite time and resources are spent on highly manual, administrative tasks. Legacy TPRM doesn't scale with your business, makes it hard to effectively leverage security data beyond the traditional questionnaire, slows down the process, and creates vendor fatigue.

But advances in AI are modernizing TPRM by combining risk management workflows with automation to accelerate assessments for buyers and vendors. AI-first TPRM makes it possible to:

- Automatically source control-specific, context-rich answers to security questions from audit reports, certifications, or previously completed standards and questionnaires in minutes.
- Leverage Large Language Models (LLMs) to understand question intent, allowing you to assess vendors using the framework of your choice—including customized questionnaires—against the security information you have. This reduces or even eliminates the need for tedious back-and-forth.
- Dramatically reduces sales and procurement cycles so buyers get the solutions they need and vendors close more deals in a fraction of the time.

Given the challenges they face, it's no surprise that survey respondents are looking to AI to play an important—and growing—role in modernizing third-party risk management. In this section, we'll look at the trends driving this ongoing transformation.

Creating Impact

Building the Discipline of AI-Based Vendor Assessments

The shift toward AI in TPRM is a work in progress; currently only 4% of companies have made the full transition to an AI-first, modern approach. But there are clear indications that momentum is building for the use of AI in both the TPRM assessment and response processes. Here's what survey data is telling us about this ongoing evolution.

Key Trends

Assessment use cases for AI are emerging. 59% of companies believe that AI is the most important trend impacting the future of TPRM (up from 51% last year), and they're already starting to use it:

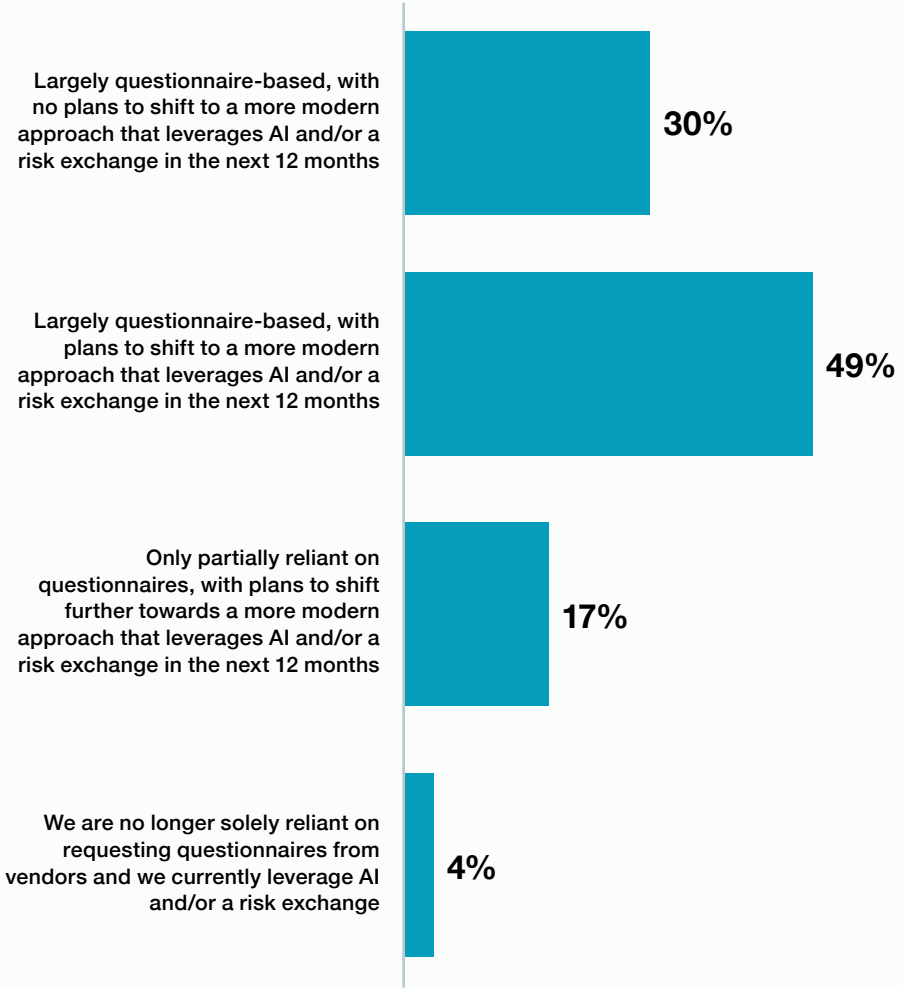
- 57% of companies are currently using AI in their assessment process, while another 40% are either currently testing it (or plan to in the next 12 months).
- 40% of companies report using AI to identify specific control gaps, data points, or evidence in vendor documentation.
- 94% of companies would be willing to use AI to summarize detailed security documentation such as a SOC 2 audit report or completed questionnaire.

Process is evolving in step with adoption. Companies are generally taking a detailed approach to rolling out the use of AI across the business:

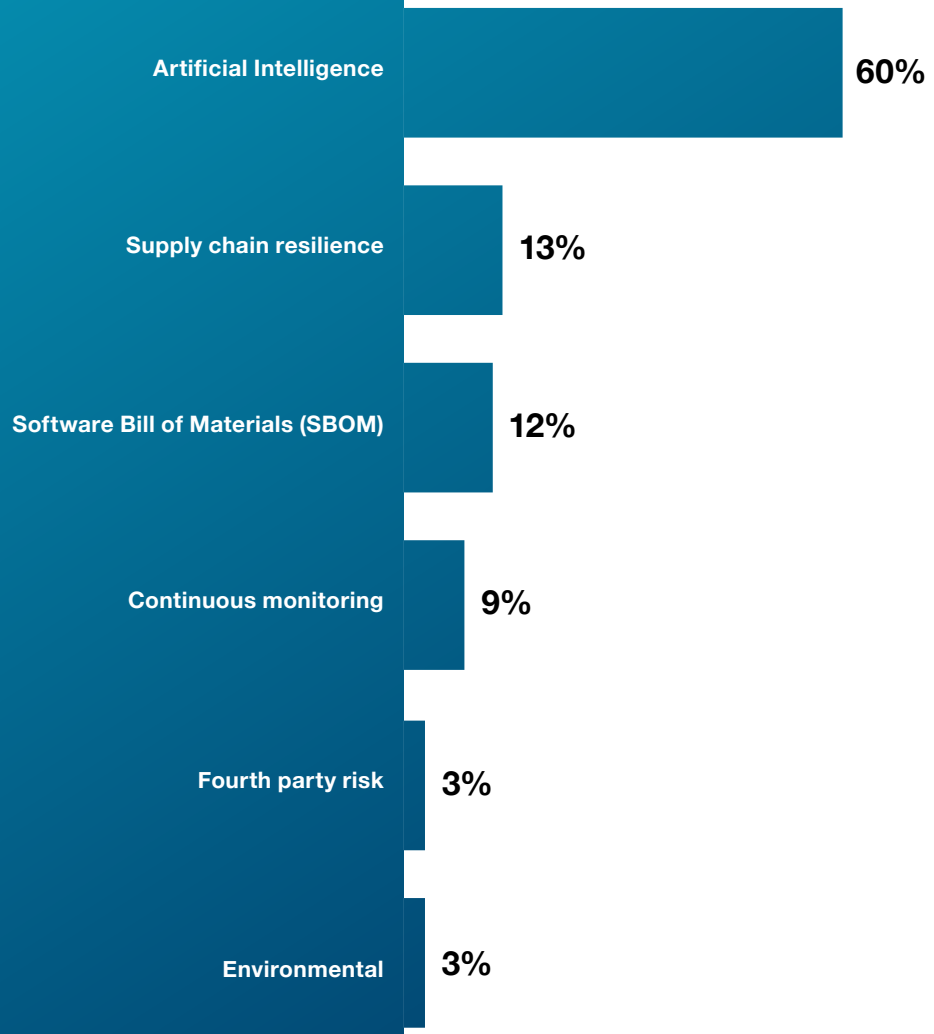
- 90% of companies have a policy in place governing the use of AI or AI-enabled technology
- 85% of companies also have an AI governance and security committee in place that must approve all uses of AI tools

Vendors are seeing the value, too. 69% of vendors believe that AI will have a "significant impact" on their assessment response process in 2025; 85% of vendors are either currently using, testing, or plan to test AI for the response process.

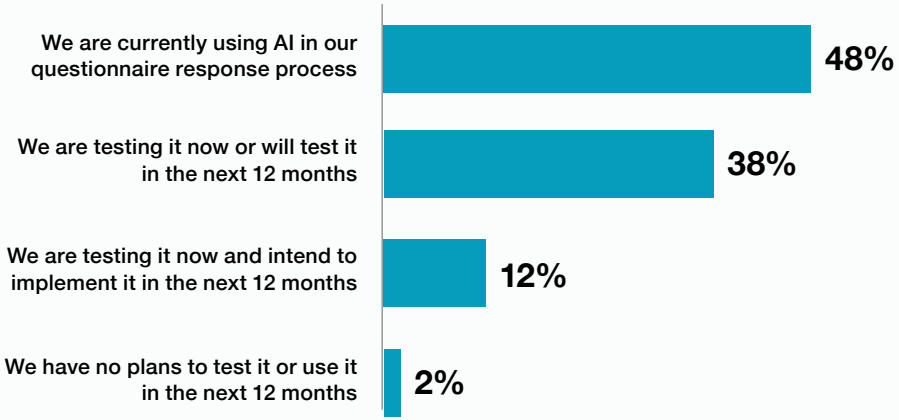
Which of the following best describes the state of your third-party risk management program?



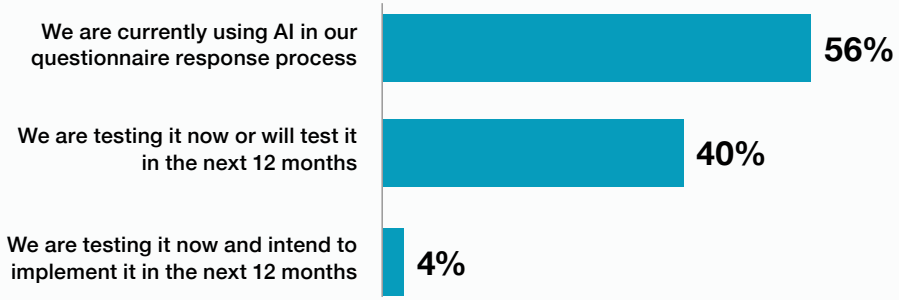
What is the most important current trend impacting the future of third-party risk management?



Which of the following best describes how you plan to leverage Artificial Intelligence in your security questionnaire response/customer trust process?



Which of the following best describes how you plan to leverage Artificial Intelligence (AI) in your vendor assessment process?



AI at Whistic

Delivering Impact for Buyers and Sellers

As our survey data shows, AI is by no means a universal feature of TPRM programs yet. But the industry is trending in that direction because of the central tension at the heart of legacy TPRM between high demand for fast vendor services and the time constraints of manual, questionnaire-dependent vendor assessments.

AI has the potential to resolve this tension, though not all AI is created equally. AI can't be an afterthought in your TPRM process; to see the greatest value, AI should integrate seamlessly into your workflow across the entire assessment process. This transforms questionnaire-driven workflows into AI-first workflows for a modern approach. This makes it possible to:

Improve the efficiency and pace of your TPRM assessments. Vendor risk teams are growing, but they're still falling behind demand. AI automation amplifies the impact of your team and greatly improves their capacity and efficacy.

Conduct all the assessments you need to. Stop cutting corners on the number of vendors you need to assess and exposing your business to unnecessary risk.

Reduce costs. Reduce the time per assessment to minutes, making it possible to accomplish the same work with a fraction of the resources.

Achieve more in-depth insights. It's clear that assessment teams are eager to use a wider range of security data to make smarter purchasing decisions. AI makes it possible to extract fast, rich insight from a broader range of sources (such as Trust Centers, exchanges, audit reports, certifications, and previously completed questionnaires).

Increase risk mitigation efforts. The time and money saved by replacing manual assessments can be reallocated to actually managing risk (instead of managing questionnaires).

Whistic's AI-first platform is integrated with your workflow, helping both buyers and vendors make the transition to modern TPRM. Here's how it works for both sides of the assessment process.

Assessment Copilot

Powerful, Automated Vendor Risk Management

The bedrock of Whistic's approach is our suite of AI capabilities called Assessment Copilot, which combines three foundational tools to automate, expedite, and enrich vendor security assessments.

Vendor Summary

The advanced machine learning and LLMs in the platform make it possible to assess any security documentation you have against the specific controls or standards you choose—without manual steps. This removes the bottleneck of the questionnaire-only approach to assessments by using the data you can collect most easily to begin your assessment.

The resulting summary comes complete with specific citations for every answer, a confidence score that explains the rationale of AI responses, and the ability to dive deeper into documentation if further clarity is needed. Whistic AI is the most accurate in the industry, and it will not invent answers. If security queries remain after completing the summary, Assessment Copilot will create a much shorter questionnaire for your vendors, greatly reducing their burden and increasing the likelihood of a prompt response.

SOC 2 Summary

82% of companies utilize a SOC 2 audit report as a part of their assessment process. But combing through hundreds of pages of reports for specific evidence is time consuming. SOC 2 Summary distills full reports down to 5-page summaries aligned to your specific security controls, surfacing the details you need automatically. It's also useful for reporting internally or sharing with senior stakeholders.

Vendor Insights

This capability makes it possible to query your entire vendor inventory at the same time, rather than doing so vendor-by-vendor. This can be especially useful when a new Common Vulnerability arises. With Vendor Insights, you can find out which of your vendors might be impacted by the incident and trigger an appropriate reassessment.

Whistic Trust Center

AI-Powered, Proactive Customer Trust

AI is not just for buyers. The Whistic Trust Center leverages AI capabilities to automate the response process, so you can respond to more requests, ease the burden on InfoSec, and close deals more quickly.

Knowledge Base

A single repository for all your security documentation, certifications, and completed questionnaires, Knowledge Base centralizes your complete security posture—no more running around from spreadsheet to spreadsheet, system to system, or just pinging InfoSec for an answer. Access to Knowledge Base is also controlled, so sales teams can be empowered to share the right information without creating an InfoSec bottleneck

Smart Search

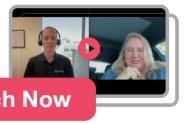
This allows you to query the information stored in your Whistic Knowledge Base, further empowering self-service for Sales or support teams to respond to customer security questions accurately. Queries can come directly from the questionnaires your customers use to assess you.

Smart Response

This capability works with Smart Search to provide context-rich answers to even customized questionnaires, complete with citations and confidence scores. Simply upload the questionnaire and Smart Response does the rest automatically. You can also audit the AI responses to ensure accuracy, and once you've approved an answer, it's added to your Knowledge Base to improve speed and accuracy on your next assessment.

Want to Learn More?

Learn more about Whistic's approach to AI
from Whistic's CEO and Principal Product Manager in this "Ask Me Anything: AI in TPRM" on-demand webinar.



Watch Now

The Survey Data Is In

Whistic's AI-First, Modern Platform Puts the Impact of TPRM in Your Hands

If you're like the companies we surveyed this year, you're facing some difficult challenges in your TPRM process: increased demand, higher risks, and costly resources that still aren't helping you meet your security, compliance, or growth goals.

That's not the kind of impact that works for your business.

At Whistic, we believe that the impact of TPRM should be experienced as greater ROI; better, faster decisions; and improved risk outcomes. Our AI-first approach integrates seamlessly with existing workflows in the assessment process, so you can assess all the vendors you need—and save your resources and investment for higher-impact risk management actions.

We also make it easier for vendors to respond to more customers in a fraction of the time, improving their own experience while building a stronger foundation of trust with consumers.

Don't let TPRM have a negative impact on your business. If you're ready to move past legacy TPRM and truly take control of risk, schedule some time with our team of experts. In 30 short minutes, we'll walk you through our platform and approach so you can experience the Whistic difference for yourself.

Schedule a Demo

whistic