whistic

2024 Third-Party Risk Management Impact Report

Table of Contents

Introduction:
TPRM Impact Report

Third parties and vendors empower our organizations more than ever, creating an ecosystem that makes it easier to collect, analyze, and act on key insights; helps us achieve greater efficiency and effectiveness; and makes it faster and simpler to scale our businesses.

But for all the benefits, third-party relationships also come with risk. More vendors means more access to critical systems and data, more vulnerabilities to a breach, and more regulatory pressures. And as that ecosystem grows, managing it becomes increasingly complex. Even knowing with certainty the number of vendors you work with can be a challenge.

Third-party risk management (TPRM) is the process of assessing, categorizing, and monitoring these complexities so your business can make confident investments in the technology, solutions, and services you need to thrive. TPRM requires a strategic approach, executive or senior-level sponsorship, cross-functional collaboration, and the right resources and systems.

In short, the impact of third-party risk management goes beyond the threat of a breach—it's felt every day, across the business.

Each year, Whistic surveys more than 500 Information Security and Risk Management professionals to understand the scope of this impact. The 2024 Third-Party Risk Management Impact Report provides timely benchmarking on:

- How your peers build and execute their TPRM programs, including the resources they dedicate, the time spent assessing vendors, the solutions they choose, and the challenges they face
- How your vendors and third-parties respond to security assessment requests and the ways it affects their strategies and operations
- How both sides of the third parties ecosystem are planning for the future, including the ways Artificial Intelligence is impacting near-term investments

Read on for the full analysis and key findings from the 2024 Third-Party Risk Management Impact Report.

Insight from the Experts:

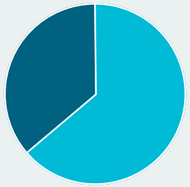
Methodology for the 2024 TPRM Impact Report

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 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 **532** InfoSec and Risk Management professionals

100% of those surveyed have decision-making and budgetary oversight for TPRM, VRM, and Customer Trust

36%
are responsible for either conducting security assessments or responding to assessment requests



64%
are responsible for both conducting security assessments and responding to assessment requests

23%
represent companies with 1-500 employees

47%
represent companies with 500-1,000 employees

30%
represent companies with 1,000-5,000 employees

Immediate Impact

A Current Snapshot of Third-party Risk

In their annual "Cost of a Data Breach" report, IBM found that the average cost of a data breach in 2023 was $4.45M per incident. And that's merely the financial fall-out—when taken with the reputational harm to your brand and an overall lack of consumer trust, the true cost of a breach is even greater.

Whistic survey data paints a clear picture of the important role that strategic third-party risk management must play in preventing and mitigating the impact of a security breach.

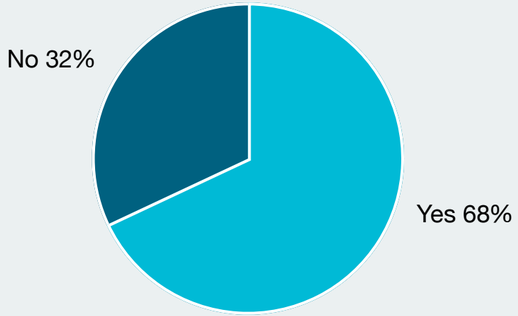
Key Trends

Security incidents are on the rise—68% of respondents indicate they have experienced a breach in the last three years; that's an increase of 13% since 2023.

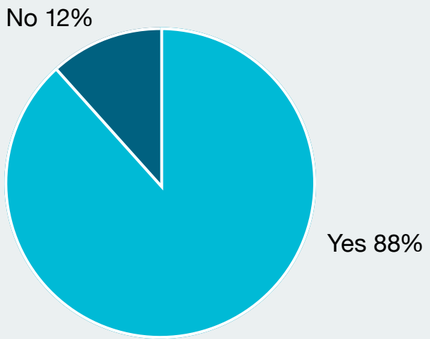
Third-party vulnerability is a huge (and growing) factor—88% of companies surveyed report that a compromise in their vendor supply chain was the cause of their breach, compared with 77% last year.

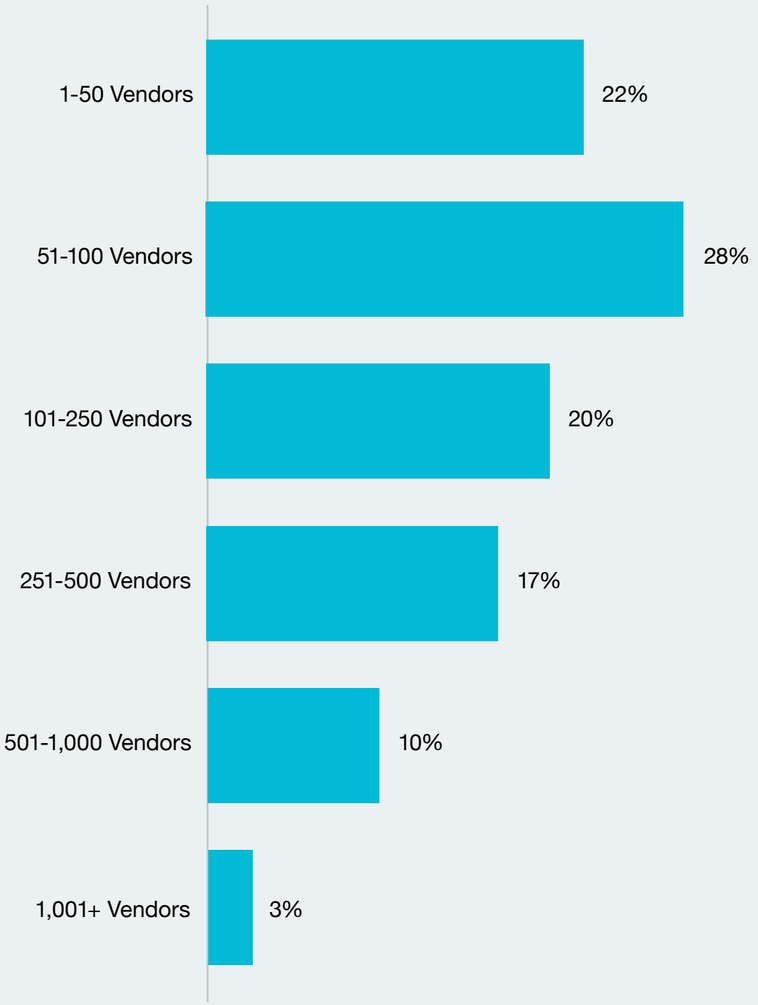
Growing reliance on third parties—In 2024, 50% of our survey respondents report working with more than 100 vendors, up from 38% of companies that had 100 or more vendors in 2023.

Has your organization experienced a data breach in the last three years?



Was the breach a result of a compromise in your vendor/third-party supply chain?





Key Takeaways

Vendors play an increasingly large business role. The average company in our survey works with 237 or more vendors. That is an enormous ecosystem to manage, suggesting that an audit of third-party relationships may be an important first step in strong TPRM.

Third-party risk is accelerating. It's no surprise to see a corresponding increase in total breaches as the threat surface grows. But it's alarming to see the percentage of those breaches originating with a vendor also increase—suggesting vendors may pose a larger risk than before.

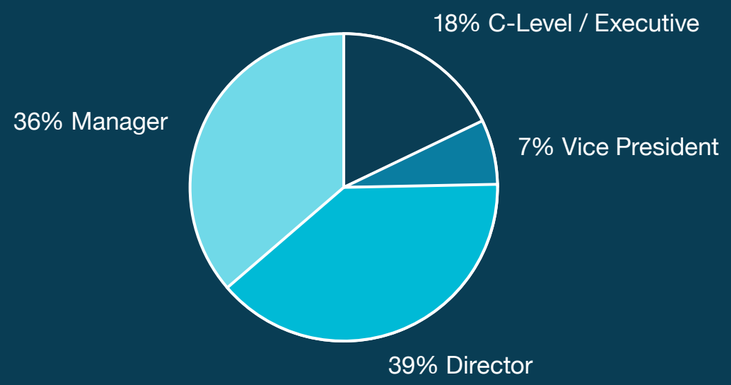
Possible causes for the surge. The increased rate of third-party related breaches points to a confluence of possible factors, including:

- More sophisticated threat actors
- New or emerging vulnerabilities across digital supply chains
- Less rigorous TPRM from buyers and customers, leading to greater risk
- Onerous burden on vendors during the security assessment process, leading to less transparency around security posture

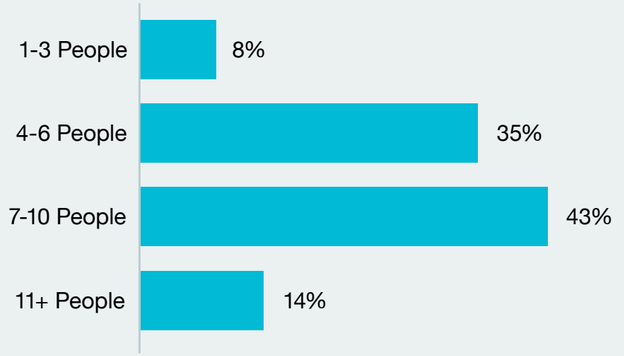
The “Who” and 'How” of
TPRM in 2024

To understand the overall impact of TPRM on the business, context is important. There is no “one size fits all” when it comes to third-party risk management—every company’s vendor needs and resources are unique. In order to capture this context, we asked survey respondents about the tactical and strategic decisions they make in building, leading, and supporting their vendor risk programs.

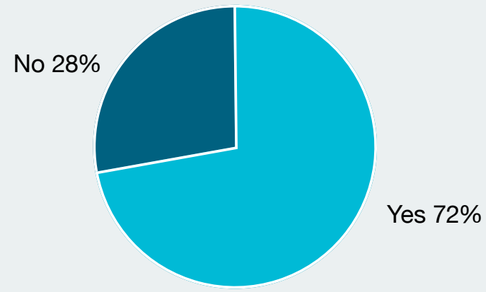
What best describes the scope of your current role?



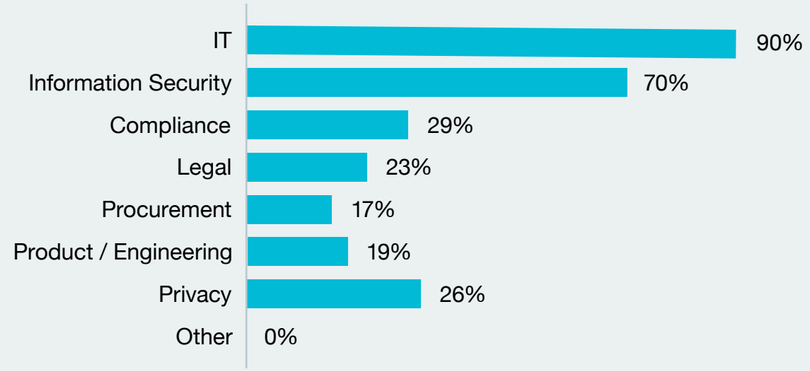
What is the size of the team in your organization involved in conducting vendor assessments?



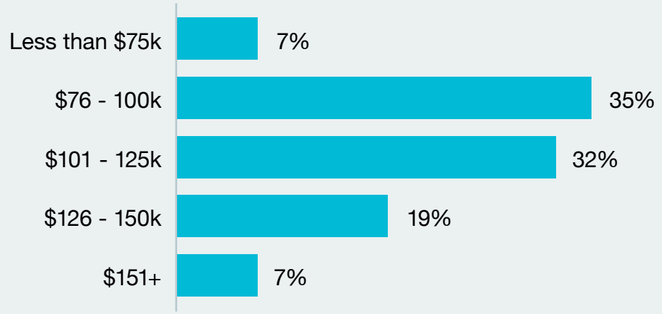
Do you plan to hire someone to assist you in conducting vendor assessments in the next 12 months?



Which of the following teams are involved in conducting a vendor security assessment at your company (select all that apply)?



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



Key Trends

More senior-level engagement in TPRM—100% of respondents in this year's survey hold leadership positions with oversight for TPRM, primarily at the manager and director level.

Lean teams are the norm—86.5% of companies surveyed have a TPRM team of 10 or fewer individuals. For these companies, the average team size is 5.6 people.

Doing more with less—Each member of these same teams is taking on vendor assessment responsibilities for an average of 36.7 vendors; this number does not include new vendors that are added or assessed during the purchasing/procurement process.

Headcount is a major investment—The average total annual compensation to add to your team will run you $109K in 2024.

Privacy teams play a larger role—This year, 26.13% of companies include their Privacy team in the TPRM process, surpassing Procurement and Legal as a critical partner in vendor risk.

Custom questionnaires remain integral—Roughly 74% of respondents say that a customized questionnaire is part of their standard assessment process (while only 19% rely on standard frameworks alone).

Key Takeaways

TPRM is increasing in complexity. Companies are involving more business units/teams in the VRM process, utilizing more technology to support the process (86% are using some kind of purpose-built software), and asking more from their TPRM teams. These factors place unique pressures on the business, including:

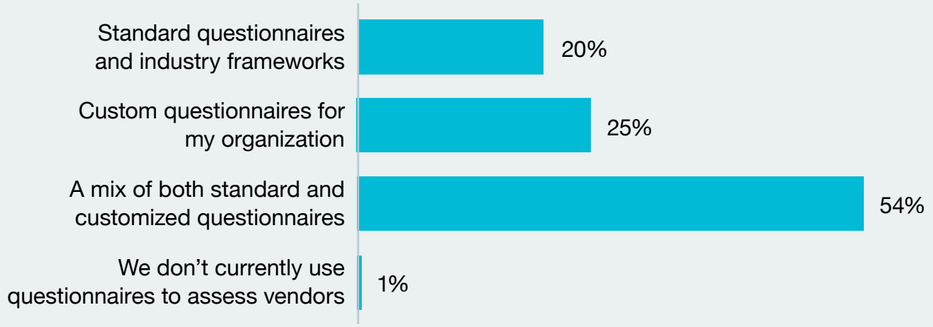
- The need for greater collaboration and strategic coordination among business units
- More technologies to manage, secure, and pay for (and more vendors to assess)
- More entry points for risk and a need for greater data-management oversight
- Existing resources stretched thin, which could lead to the neglect of other business-critical activity or compromised risk-management practices

TPRM is increasing in strategic importance to senior leadership. In response to this increased complexity, executive sponsorship/ownership of TPRM is increasing. All respondents hold leadership positions in their organization, including more than 18% C-level.

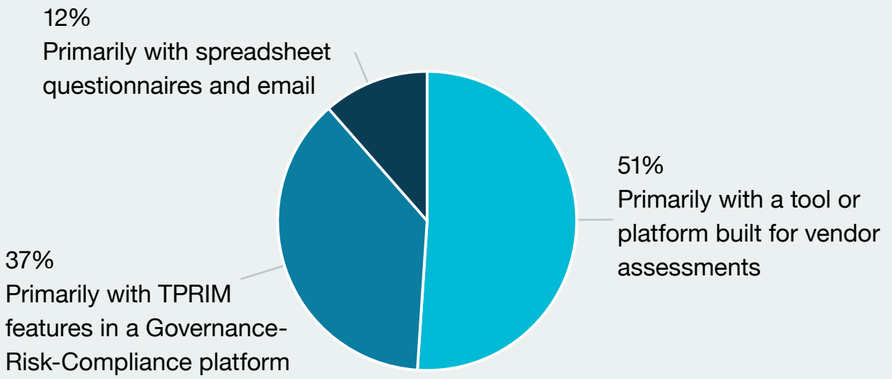
TPRM teams need help. Most organizations surveyed employ small-to-medium-sized teams handling large numbers of vendors. 80.1% of all respondents also use some kind of customized questionnaire in their assessment process, which increases the amount of manual work per assessment (which in turn leads to longer assessment times and greater potential for human error).

But will they get it? The use of TPRM software increased nearly 20% over the last year, which suggests a move toward automation that could spell relief for over-burdened teams. But while companies express an interest in adding headcount, a steep price tag during times of budgetary tightening might put hiring out of reach in the near term.

What types of questionnaires do you use to assess vendors?



How does your company currently conduct vendor assessments?



Vendor Security Assessments:

Impact on Buyers and Customers

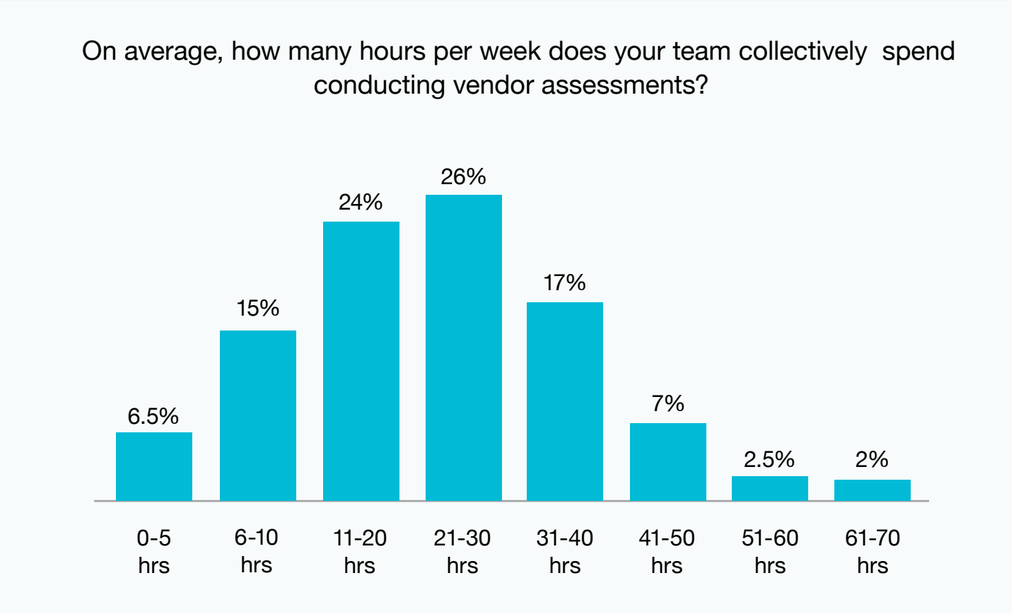
As we've seen, third parties and vendors are a bigger part of business success than they've ever been. Security assessments allow companies to make informed decisions about the types and degree of risk they are willing to take on when adding these products and services to their ecosystem.

TPRM's ongoing shift in strategic importance—as evidenced by the growing complexity and increased engagement from the C-suite—are having an impact on the time and resources necessary to execute vendor assessments, as well as on the decision-making capacity of the business. In this section, we'll look at survey data pertaining specifically to the vendor assessment process.

Where Does the Time Go?

Understanding the Impact of Vendor Assessments on Resources

More vendors, more opportunities for risk…and more at stake. That's the pressure facing third-party risk teams and the business units they empower. In this context, it's helpful to understand the time demands (and time constraints) you face when honing your TPRM program.



Key Trends

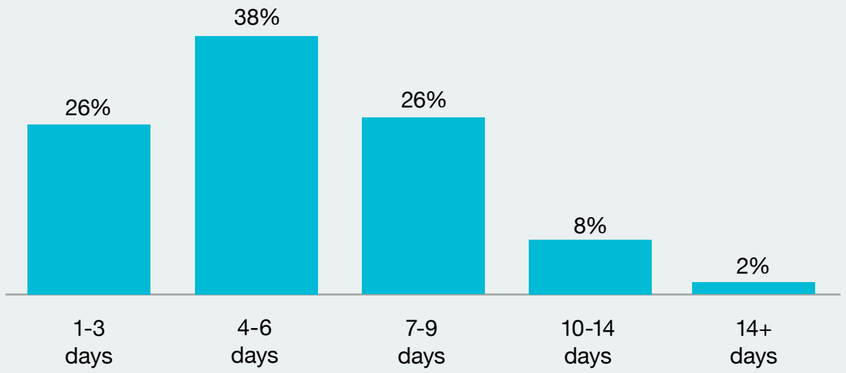
TPRM is on the clock—54.7% of respondents spend more than 21 hours every week on the vendor assessment process. The average team spends 23.88 hours every week on assessments, while nearly a third of all companies spend more than 30 hours each week.

The waiting is the hardest part—While gathering information and reviewing security documentation are time-consuming, assessments can slow to a crawl waiting on responses from vendors. 74% of companies wait more than 4 days to hear back from vendors; 36% wait longer than a week.

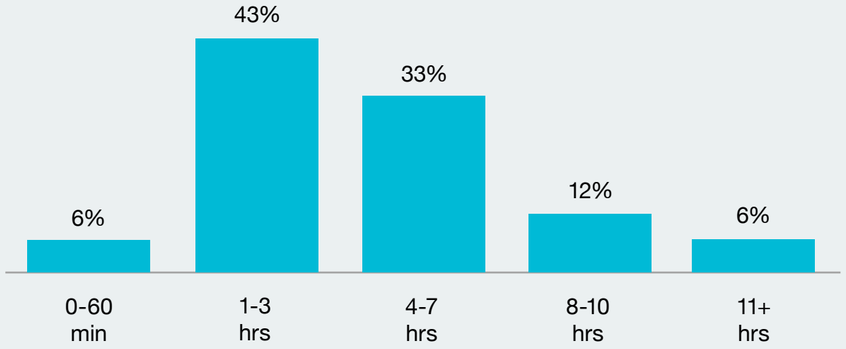
Additional factors add time, but are hard to control—Vagaries in the assessment process are disruptive because they are difficult to plan for, and often add hours or days per vendor:

- High-risk vendors add 1-7 hours per assessment for 81.22% of companies
- Requests for follow-up clarification or additional vendor info add 4-10 hours of time per assessment in 65% of cases
- 87% of respondents do manual updates of customized questionnaires more than once a year—with 21% updating them monthly
- On average, survey respondents experienced 4 security incidents per year (like Common Vulnerabilities and Exposures) that trigger and assessment or reassessment; each of these takes an average of 15.23 hours.

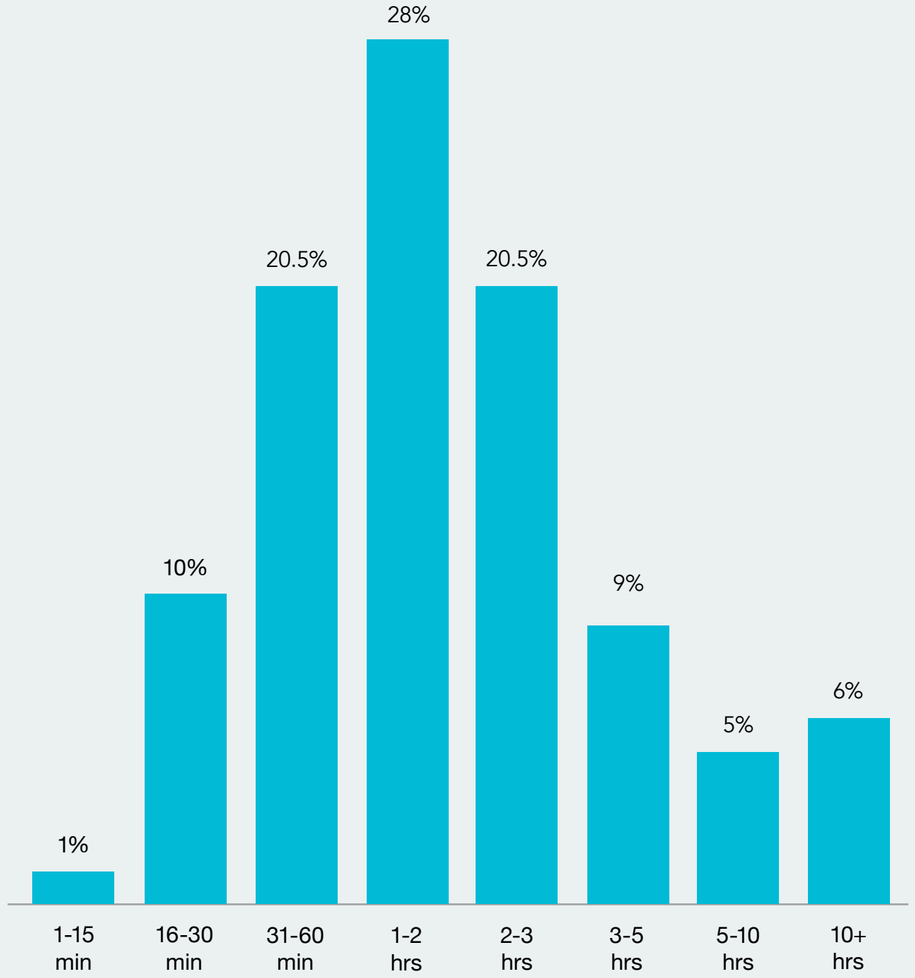
On average, how many days does it take for a vendor to respond with complete information on an assessment request?



On average, how much time does your organization spend per vendor getting clarification after your initial assessment, gathering additional documentation, creating remediation plans, and chasing down responses from the vendor?



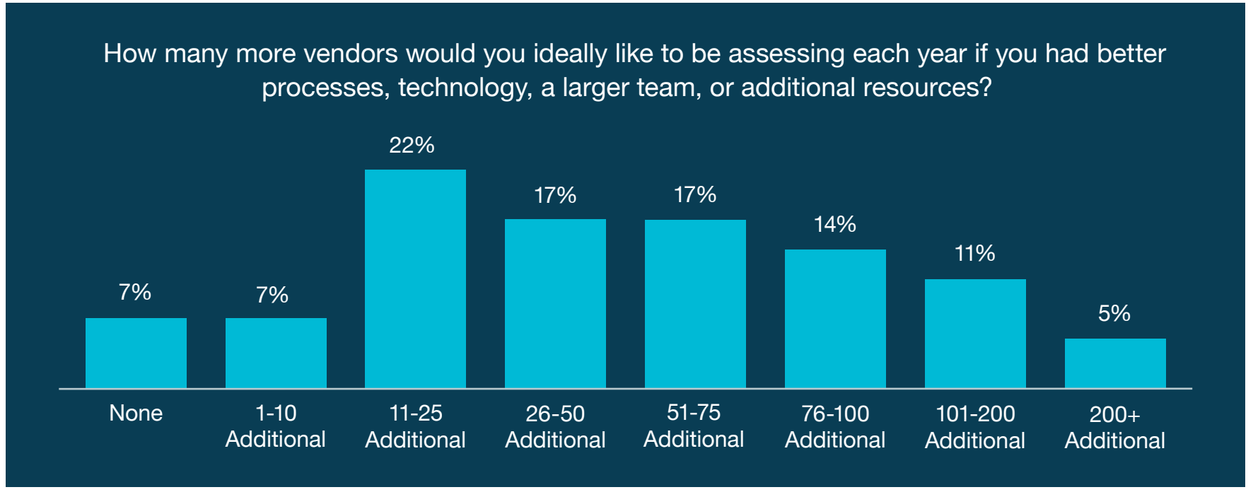
On average, how much time does your company spend per vendor gathering intake information, determining inherent risk, and selecting the type of assessment needed for each vendor?



Quantity or Quality

Is the Time Burden Leading to Corner-cutting on Vendor Security?

Time and resource constraints on TPRM teams are a fact of life for most organizations. But are these factors impacting the quality of the assessment process? Our survey data suggests that it's having a real effect on the assessment choices companies are making.



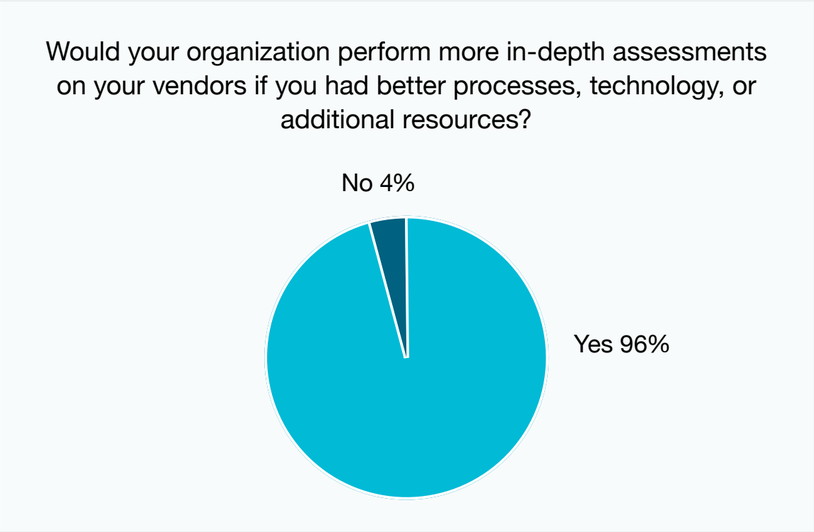
Key Takeaways

There is a clear appetite for richer, more far-reaching vendor assessments, but a lack of resources has lead to difficult choices for TPRM teams. The high number of security breaches that originate in the third-party ecosystem (87.5% of all incidents) may be in part explained by this kind of costly compromise.

The demand for vendor solutions and services seems to outweigh the need for more thorough vendor assessments. This approach requires careful cost-benefit analysis comparing the impact of delayed solutions against the impact of a breach.

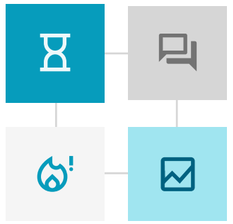
In general, this data suggests that companies are taking on greater risk than they would prefer in order to meet demand without additional resources. While this might accelerate the assessment process, time and costs may only be deferred to risk management, continuous monitoring, and mitigation. Where will these resources come from?

Collaboration and trust between vendors and their customers is more important than ever. Transparency from vendors can expedite the assessment process, making it easier to conduct detailed reviews. And buyers can meet their vendors halfway by seeking opportunities to automate and stretch the impact of their teams.



Responding to Assessments:

Impact on Vendors and Customer Trust



Third-party risk management processes also have an enormous impact on…well…third parties. Responding to security questionnaire requests from prospects and customers can be a complex and time-consuming challenge to vendors for many reasons:

- Security documentation is often decentralized or highly controlled, which makes InfoSec the only source of truth for the organization. This can lead to a bottleneck—not to mention keeping InfoSec from other business-critical activities.
- Out of necessity, Sales often plays a role in the questionnaire response process, taking time away from closing deals.
- Customers are utilizing more TPRM technology (86% are using some kind of tool), but that means vendors often must manage requests, communication, licenses, and log-in info for dozens of different systems to accomplish the same task.
- Poring over security documentation can take hours and lead to fire drills when a deal needs to close—especially if security info lives in manual spreadsheets or answer libraries.
- Total transparency can still be viewed as a risk, limiting the amount of proactive sharing that can safely be done to accelerate the process.

And sometimes, the ultimate outcome is that a vendor simply doesn't respond to a request at all, shifting the burden of risk to their customers—or losing a sale entirely. In this section, we'll take a look at the factors that contribute to these challenges for Customer Trust teams.

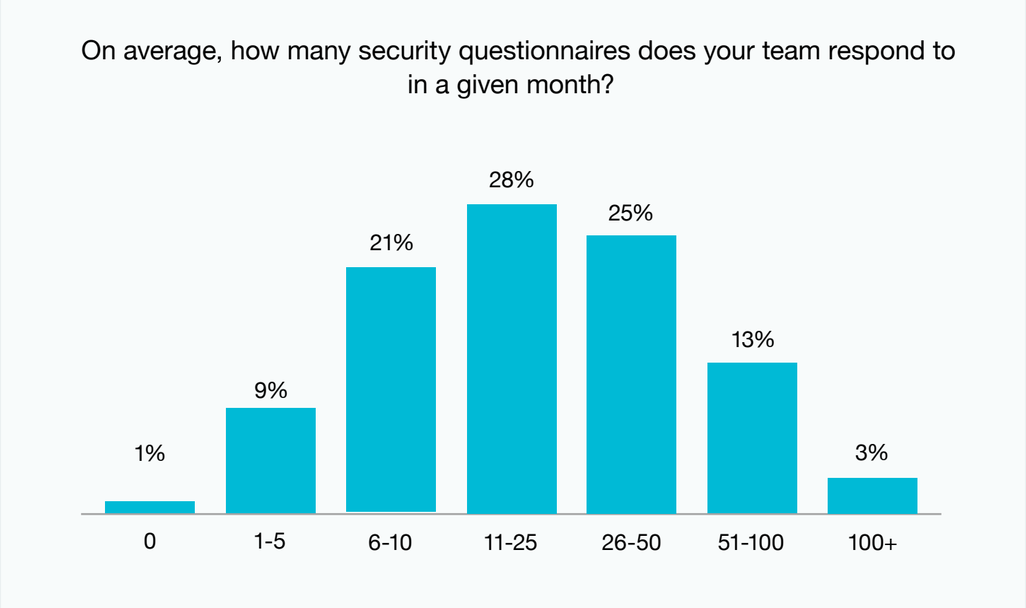
Feeling the Crunch

Balancing Time, Resources, and Consumer Expectations in Customer Trust Programs

Security is every bit as important to vendors as it is to their customers. But time is also of the essence because delays in the TPRM process can result in lost deals, lost revenue, and an erosion of customer trust.

It's a tricky balancing act for vendors. An emphasis on speed and efficiency can ease the burden on InfoSec and accelerate the Sales cycle. But our survey found that 84.5% of vendor assessments require some kind of follow-up, adding hours, days, or even weeks to the process. Speed at the expense of quality may actually cost time.

Here's a few of the factors vendors are weighing for their Customer Trust programs.



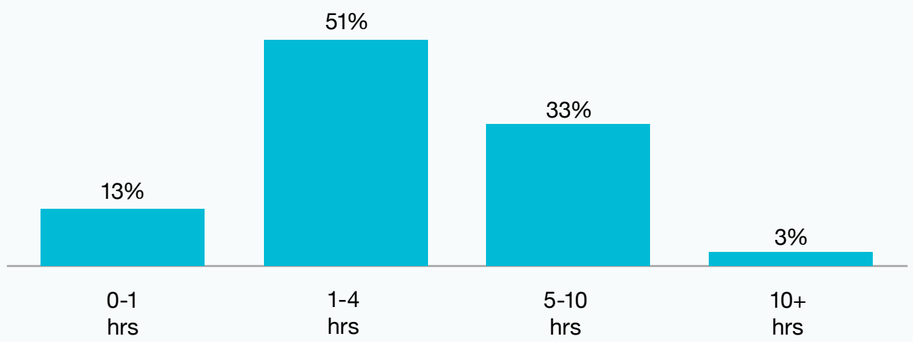
Key Trends

The number of assessment requests is rising—More than 70% of companies report responding to more than 11 questionnaire requests every month. This is an increase of 16% since last year. And 40% respond to 26 or more requests, which is twice as many as last year.

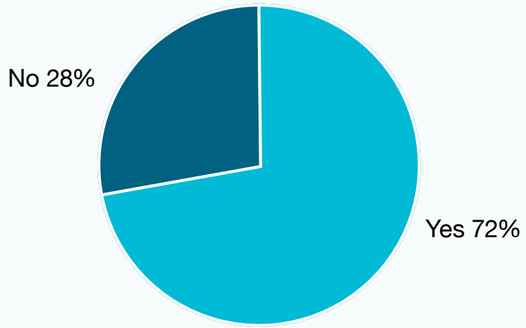
Response times are high, but also get stretched over days—83% of companies spend up to 10 hours per response, which can be a significant burden given the rising number of questionnaire responses companies now undertake. But that work is also rarely done in a single sitting, with more than 90% of companies taking at least 2-3 days to complete and return a response.

A proactive approach moves the needle—The majority of companies surveyed are able to deflect a significant portion of incoming requests simply by sharing detailed security info proactively and early in the sales cycle. This is especially true when you make the answers to standard questionnaires like SIG or CAIQ available on-demand; 95% of respondents indicate that such a standard is enough to start a thorough assessment.

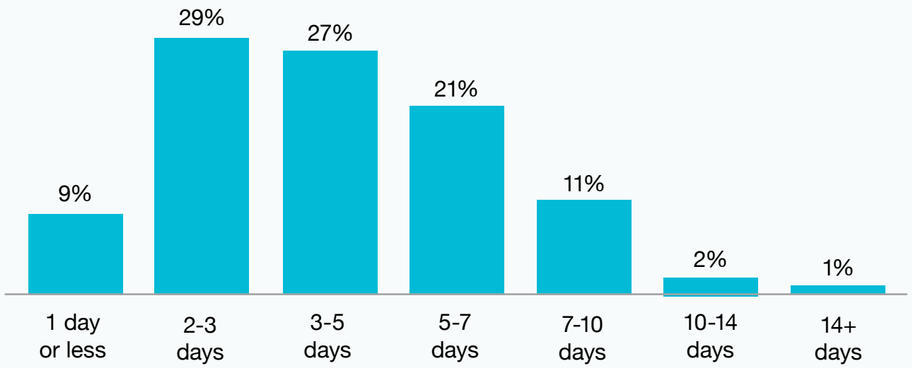
On average, how many hours does your team spend on each security questionnaire response?



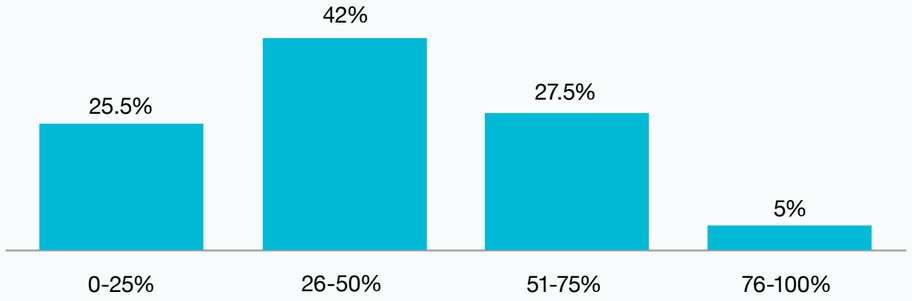
Do you currently make your security documentation available publicly to customers and prospects?



On average, how many days does it take you to return a completed security questionnaire to your customer?

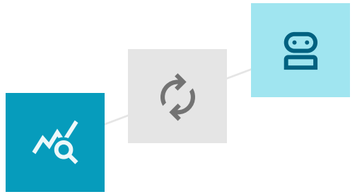


On average, what % of security questionnaires are deflected when you proactively publish or share your documentation before you receive a request from your customer?



Take Control:

Create Positive Impact with Your TPRM Program



In third-party risk management and customer trust, the impact is often felt as something reactive, something that happens to us: a business unit needs to procure new software, so TPRM must perform an assessment. Our customers can't move forward on a deal until we respond to a questionnaire. It's no wonder these activities have long been perceived as a "necessary evil."

It doesn't have to be that way.

The tide is turning, and TPRM is already beginning to be viewed as a strategic enabler. To embrace this opportunity, organizations must combine excellent process, strong leadership, and smart investment in technology. This kind of comprehensive approach can make the TPRM impact a positive one for the business. In this final section, we'll share a detailed approach to building a world-class TPRM program. This will form the foundation for more agility, greater collaboration, and increased efficiency.

We'll also take a closer look at one of the most exciting trends impacting our industry: Artificial Intelligence. When combined with great process, AI can be applied to all of the major challenges facing vendors and their customers. It's a big point of emphasis in 2024 for the companies we surveyed, and we'll share the ways Whistic is delivering on the promise of AI in our own approach.

5 Essentials for Building a World-class TPRM Program

Taking control of TPRM impact starts with the right strategy and planning. We've identified five essential elements to take your TPRM program from good to great—regardless of the size of your team or your unique assessment needs.

1 Establish program governance

Create an oversight plan for your TPRM program to determine lines of accountability and communication while measuring outcomes with an eye toward continous improvement

- Create a cross-functional TPRM Committee. Your needs may vary, but a strong governance team may include Compliance, Legal, Procurement, IT, and business units.
- Establish key metrics to track success and develop a regular reporting cadence.
- Create defined security requirements for contract language.

2 Create a vendor inventory and vendor profiles

Having an up-to-date, centralized picture of your entire vendor ecosystem makes assessments simpler to execute. Vendor profiles augment your inventory with all the information necessary to evaluate risk, including:

- Necessary security documentation, like SOC reports or certifications
- Vendor contracts
- Documentation for any issues to monitor with a given vendor

3 Develop risk ranking criteria

Risk ranking is a straightforward methodology for classifying levels of inherent risk consistently across vendors, making it easier to compare and understand the risks you face. Strong risk ranking takes into account:

- The kinds of data vendors or third parties will have access to (PII, intellectual property, financial records, etc.)
- The volumes of data you'll be sharing with the third party
- The systems and networks your vendors will have access to
- The services your vendor provides to support any regulatory or compliance requirements
- How critical the vendor is to your business operations
- Any specific factors that impact your unique risk profile

4 Calibrate your assessment process to risk levels

The level of risk a vendor represents determines the kind of assessment that is appropriate. By matching the right assessment with the right risk profile, you can maximize efficiency and increase the velocity of your program. The full assessment process should:

- Clearly explain the purpose, scope, and context to your vendor, as well as detail specific areas of focus aligned to your unique business needs
- Identify control issues and make clear recommendations
- Include detailed assessment reports and a risk-management plan
- Ensure assessments are applied uniformly across your vendor inventory

5 Develop a remediation plan

Once you've defined your risk criteria and assess your vendor's security posture, it's critical to develop a management plan that allows you to properly remediate risks. Your remediation program should include:

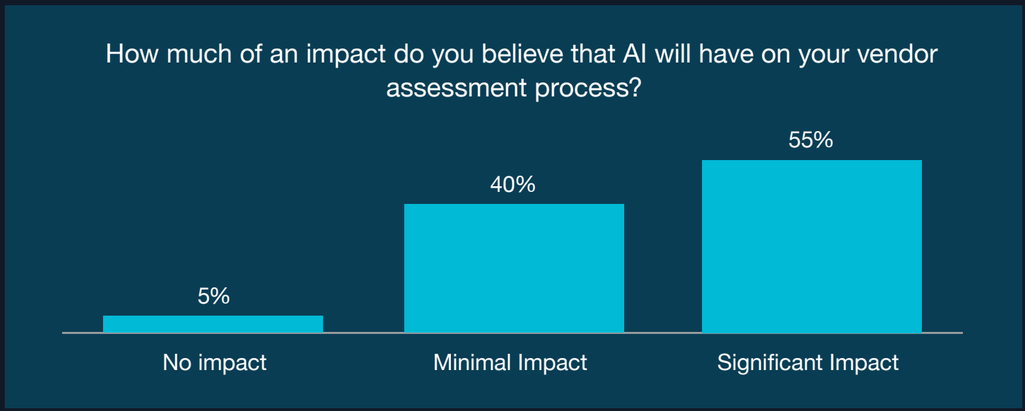
- Proper allocation of InfoSec resources aligned to risk ranking and assessment results
- Processes for reassessment of your vendors on a regular cadence
- Collaboration among business units and stakeholders to maintain visibility into your third-party landscape and reduce shadow IT
- Clear procedures for incident response

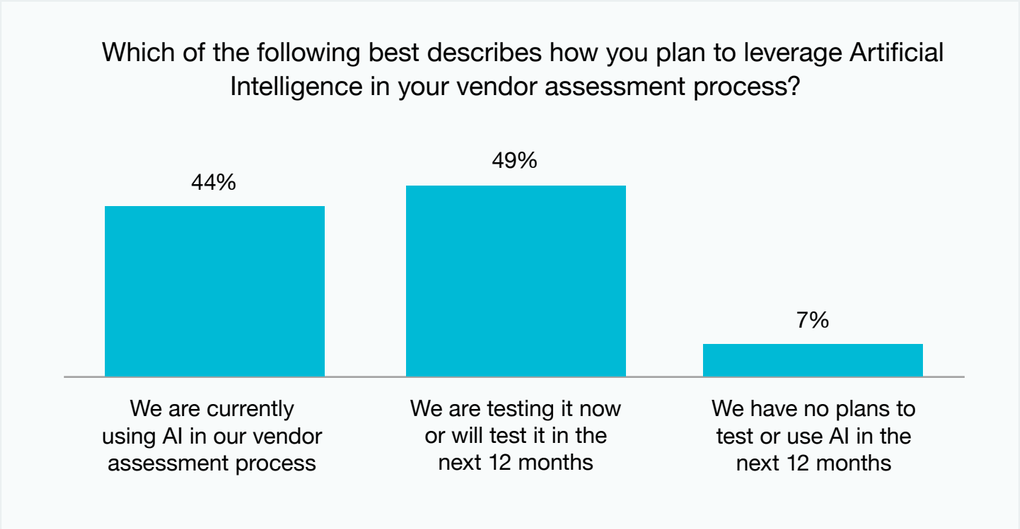
Immediate Impact

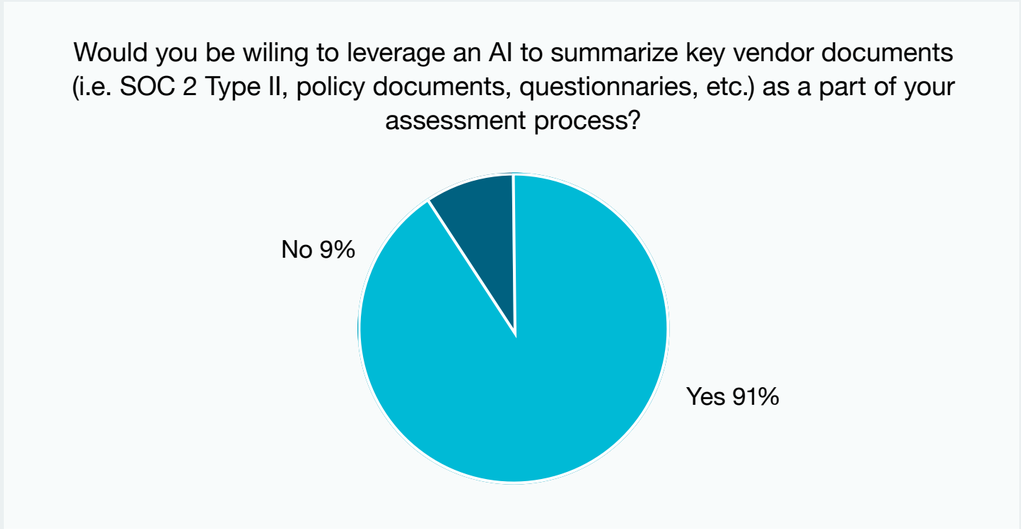
How Artificial Intelligence is Shaping the Present and Future of TPRM

AI has the potential to solve some of the biggest challenges facing both sides of the TPRM process. When we asked the companies in our survey for their thoughts on AI, the response was resounding:

- Only 5% believed that AI won't have an impact on vendor assessments or questionnaire responses.
- More than 92% of companies are currently using or testing AI in their assessment process
- More than 93% of those surveyed are currently using or testing AI in their response process

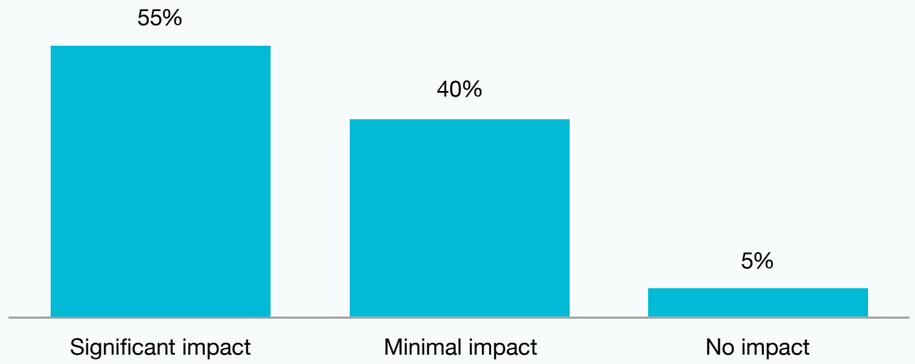




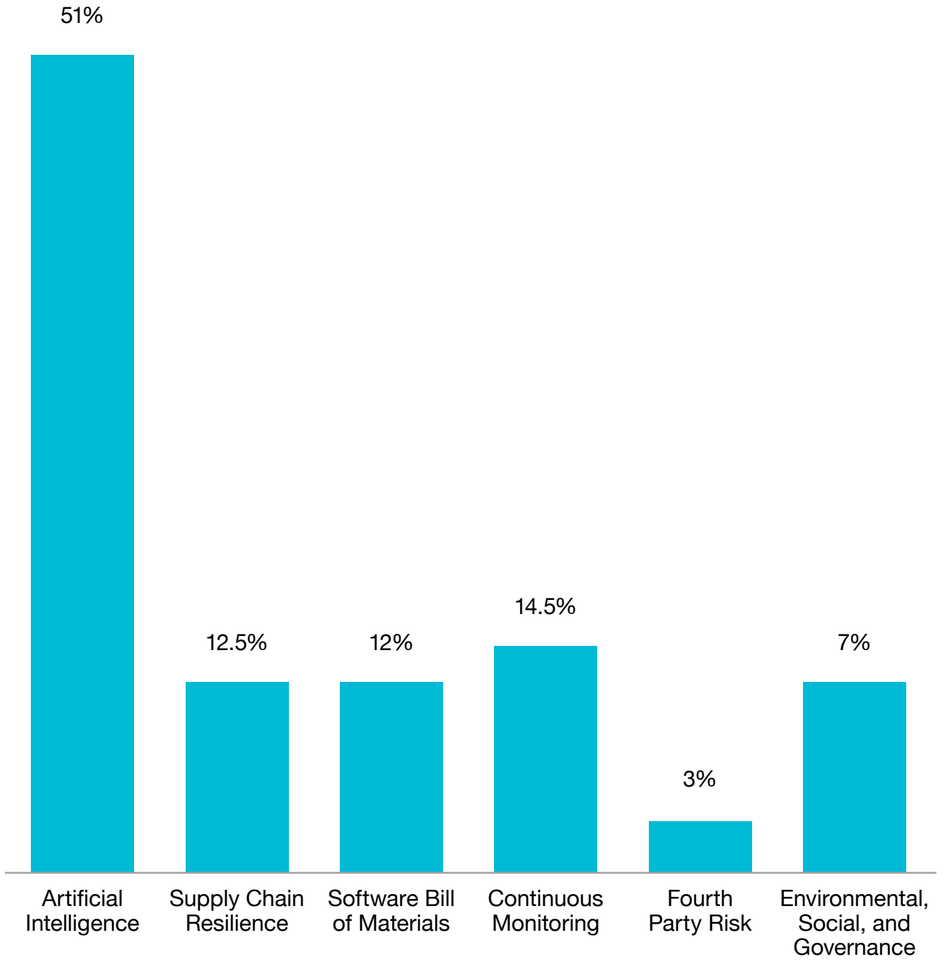


Which of the following best describes how you plan to leverage Artificial Intelligence in your security questionnaire response/customer trust process?

How much of an impact do you believe AI will have on your questionnaire response process?

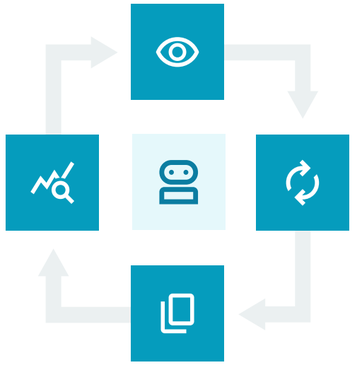


What is the most important current trend impacting the future of third-party risk management?



AI at Whistic:

Delivering Impact for Buyers and Sellers



Our survey data shows that risk management is rife with competing challenges:

- Lengthy security assessments vs. business demand for new vendors
- Possible breaches vs. resource-constrained InfoSec teams
- Questionnaire response times vs. faster sales cycles

Quality security outcomes and speed are both priorities, but our survey data suggests these are in constant competition with one another. AI resolves this contradiction by making high-quality assessments faster without additional headcount. By automating questionniare responses and providing control-focused summaries of detailed security documentation, AI:

- Allows customers the opportunity to extract control-specific answers to security questions from completed standards like SOC 2 or completed questionnaires their vendors pass along—no more cutting corners on assessments or waiting around for responses.
- Understands the intent of questions, so vendors can respond to even customized questionnaires automatically—no more multi-day delays in response times.
- Fosters transparency and empowers Sales to respond to security questionnaires without sacrificing oversight.
- Dramatically reduces sales and procrument cycles—buyers get the solutions they need faster and vendors close more deals.

Whistic AI resolves the tension at the core of third-party risk management and helps resource-constrained risk and trust teams realize their strategic potential and deliver value to the business. On the next page, we'll show you how it works for both buyers and vendors.

Whistic Assess:
Vendor Security Powered by AI

Smart Search allows you to query the security documentation you receive from vendors for specific, context-rich answers to your questions—complete with confidence scores and citations. This means that if you don't get a response to your customized questionnaire or you need clarification, you can find the answer without the need for frustrating back-and-forth or lengthy delays. And there's no more cutting corners, because you know you can always get every answer your team needs to make great, security-first decisions.

Vendor Summary allows you to apply Smart Search to your existing vendor catalog, making it easy to find answers or exceptions during regular reassessments—which means you can more easily stay up to speed with vendor security even as new threats emerge. This is especially helpful when new Common Vulnerabilities and Exposures arise.

SOC 2 Summarization allows you to organize hundreds of pages of SOC 2 reports into concise summaries based on your specific requirements, controls, and exceptions, so you can dedicate your limited resources and time to the risks that truly matter most for your business. These document summaries are also great shareable executive reports for senior management and the C-suite.

Trust Catalog collects trust center info from thousands of vendors, allowing you to query for only those vendors that meet your security requirements. You can do this early in the purchasing/procurement process to save time by eliminating vendors that don't meet your needs.

Whistic Trust Center:
AI-powered, Proactive Customer Trust

Knowledge Base is a single repository for all your security documentation, certifications, and completed questionnaires. Knowledge Base centralizes all your security documentation—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 queries the information stored in your Whistic Knowledge Base, futher empowering self-service for Sales or support teams to respond to customer security questions. The AI in Smart Search understands question intent, so it can even be used for customized questionnaires.

Smart Response 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.

SOC 2 Summarization isn't just for customers. If your prospect or customer is using Whistic Assess, you can simply send them your SOC 2 report and AI will take care of the rest in a one-touch assessment that's as simple as clicking a button. But you can also apply SOC 2 Summarization to your own report based on the controls and requirements of your customer, so the information you send them is catered to their needs and speeds up the entire process—so you can close deals faster and InfoSec can focus on keeping your business secure.

The Survey Data Is In:

Whistic's AI-Powered Platform Can Put the Impact of TPRM in Your Hands

In 2024, the impact of third-party risk management is being felt far beyond the threat of a breach. That would be impactful enough, but TPRM now also touches more business units than ever, has more strategic value to executive leadership and the C-suite, and fuels a growing need for third-party relationships that help to keep you competitive.

If you're like the companies we surveyed, you're facing some difficult challenges in this environment: greater demand, fewer resources, the choice between security and speed, and the pressure to close deals fast. Whistic is an industry-leading, dual-sided TPRM platform that brings buyers and sellers together in one AI-powered platform.

With Whistic, you never have to choose between a world-class security assessment and getting the tools you need, nor will you have to choose between providing excellent service to your customers and closing a deal.

If you're ready to take control of the TPRM impact, we're ready to help. Schedule a quick, 30-minute consultation with our experts and find out if the AI-powered future of third-party risk is right for you.

Schedule a Demo

Or contact Whistic today**: sales@whistic.com**