ProcessUnity

State of Third-Party Risk Assessments

2026

The Cost of the Maturity Gap

Organizations today believe their TPRM processes are mature, but the data they shared via our 2026 survey tells a different story.

Prepared in collaboration with Ponemon Institute

Table of Contents

PART 1

Introduction to the Data & the Maturity Gap

Organizations across many industries increasingly believe their Third-Party Risk Management (TPRM) programs are mature. The data in the ProcessUnity State of Third-Party Risk Assessments 2026 tells a more complex story. While most organizations have established assessment processes, policies, and frameworks, the data from our 1,465 respondents uncovers that many have not achieved true program maturity, and the gap between perception and reality is growing.

That gap has a measurable cost. Organizations are experiencing frequent third-party breaches, prolonged assessment cycles, slow vendor responses, incomplete remediation, and persistent blind spots across their third-party ecosystems. In fact, organizations report experiencing an average of 12 third-party breaches per year, signaling that third-party risk is not an edge case, but a recurring operational reality. These outcomes highlight a critical truth: having processes in place is not the same as operating a mature, scalable, and effective TPRM program.

Organizations report experiencing an average of ***12 third-party breaches per year***

Purpose of this Study

The ProcessUnity State of Third-Party Risk Assessments 2026 , based on research conducted by the Ponemon Institute, examines how organizations assess and manage third-party risk and evaluates whether current Third-Party Risk Management (TPRM) assessment programs keep pace with the realities of modern third-party ecosystems. We studied how third-party risk assessment programs are executed in practice, how long they take, how consistently they scale across vendor portfolios, how confident organizations are in them, and whether they meaningfully reduce the likelihood and impact of third party-driven incidents.

Third-party risk assessments represent a foundational component of TPRM programs. But while many organizations have formalized assessment processes, policies, and governance structures in place, this research evaluates whether those processes translate into measurable outcomes, including reduced breach frequency, improved visibility, and timely remediation of identified risks.

About the Research & Global Data Set

The Ponemon Institute surveyed 1,465 third-party risk practitioners, managers, and leaders, including IT, security, risk, and compliance professionals who are directly involved in their organization's third-party risk assessment activities. Respondents represented organizations across North America, EMEA (Europe, Middle East, and Africa), and APAC (Asia Pacific), and spanned a broad range of industries, including Financial Services, Technology & Software, Public Sector, Manufacturing, Healthcare, and others.

The survey consisted of 34 primary questions, in addition to demographic questions related to organizational size, industry, and geography. The questions examined a wide range of Third-Party Risk Management practices and outcomes, including:

- TPRM program maturity and perceived effectiveness
- Assessment timelines and resource requirements
- Vendor responsiveness and questionnaire completion
- Portfolio coverage and visibility across vendor ecosystems, including fourth-party risk
- Onboarding decisions and remediation practices
- Third-party breach frequency and impact
- Systems, tools, and budget used to support assessments

All responses were collected confidentially and analyzed in aggregate by the Ponemon Institute.

To better understand how scale, geography, and industry influence third-party risk outcomes, responses were analyzed by region, industry, and organizational size using the following definitions throughout this report:

- **Large organizations:** More than 10,000 employees
- **Small organizations:** 10,000 employees or fewer

Respondents represented organizations across North America, EMEA (Europe, Middle East, and Africa), and APAC (Asia Pacific)

The TPRM Maturity Gap

Based on survey responses, nearly half of organizations believe their Third-Party Risk Management programs are mature. Many point to standardized assessments, documented policies, defined workflows, and formal governance as evidence that their programs are working. On paper, these indicators suggest progress and control. In practice, the data tells a different story. Organizations report experiencing an average of 12 third-party breaches per year, and assessments routinely take four months or longer to complete (64% of large organizations report a four-plus month timeframe). These outcomes raise a critical question: if assessment programs are truly mature, why does risk continue to materialize so frequently?

The TPRM maturity gap highlighted in this survey represents a disconnect between having third-party risk processes in place and operating a program that consistently delivers meaningful risk reduction at scale.

KEY STAT

53% of Companies Surveyed Believe They Have Effective Third-Party Assessments

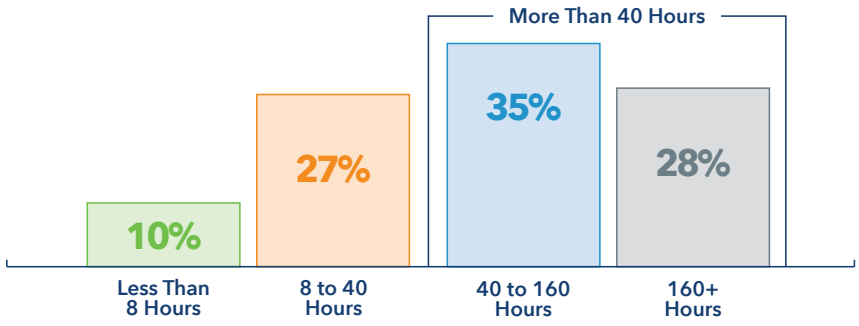
However...

ONLY 49% of Companies Surveyed Measure the Effectiveness of Their Third-Party Assessments

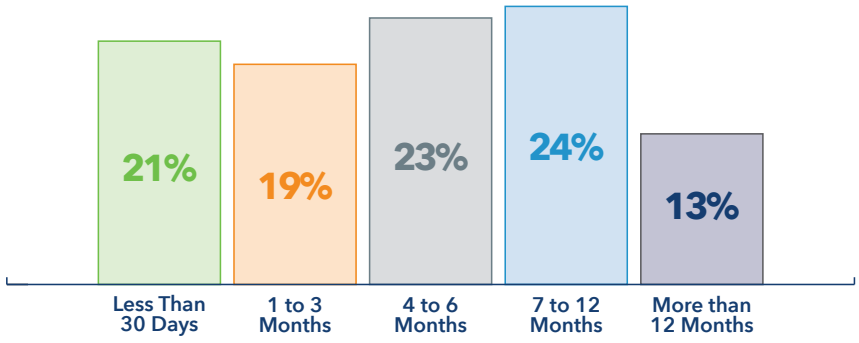
Process Maturity vs. Program Maturity

Most organizations reach basic process maturity. Teams conduct assessments, distribute questionnaires, and document workflows. Far fewer reach true program maturity, where those processes move quickly, scale across the entire vendor ecosystem, and materially reduce exposure.

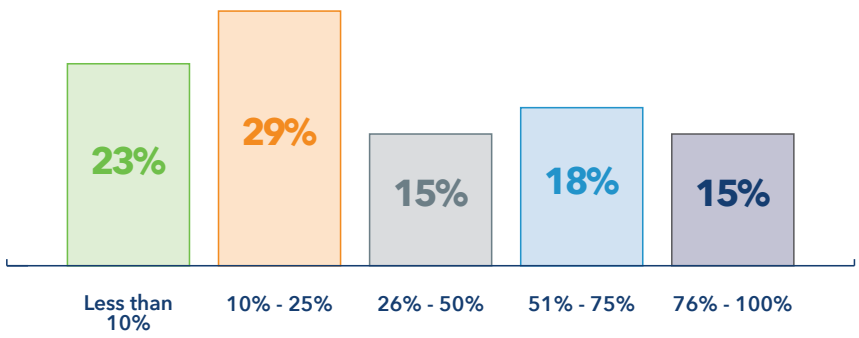
On average, how many hours of your team's time does **one** third-party assessment take?



On average, how long does it take to complete one third-party assessment (from launch to closure)?



What percent of your total third-party population do you assess? (Please select one choice only)



Focusing On Activities vs. Outcomes

The distinction matters because process maturity focuses on activities, while program maturity focuses on outcomes. A program can complete assessments, enforce policies, and meet internal and regulatory requirements, yet still struggle to prevent incidents, close remediation gaps and assessment backlogs, or maintain visibility across third- and fourth-party relationships. 63% of organizations claim a single assessment takes more than 40 hours for their team to complete over multiple months, yet outcomes do not improve as we illustrate throughout this report. This illustrates a widening gap between perception and reality.

The cost of this maturity gap is cumulative. Long assessment cycles delay risk decisions. Manual workflows concentrate effort on individual contributors rather than distributing risk ownership across the organization. Limited coverage leaves large portions of vendor ecosystems unassessed. Deferred remediation allows known issues to persist in production environments. Over time, these conditions create operational drag, increased risk, and repeated exposure.

Perhaps most critically, the maturity gap creates a false sense of confidence. Visibility can concentrate on responsive, easy-to-assess vendors, while harder-to-evaluate relationships may receive less scrutiny. Programs appear effective based on what is visible, even as material risk remains unmanaged. As third-party ecosystems grow larger and more interconnected, this false confidence becomes increasingly dangerous.

Closing the TPRM maturity gap requires a shift in how organizations define success. True program maturity depends on the ability to:

- Move faster without sacrificing rigor
- Scale assessments intelligently across the vendor population
- Reduce reliance on manual effort
- Evaluate effectiveness through measurable outcomes rather than process completion

The sections that follow explore how this gap manifests across assessment execution, vendor engagement, remediation practices, and visibility, and explain why organizations must close the gap to manage third-party risk in today's operating environment.

PART 2

The Ten Findings That Will Reshape Your Approach to Third-Party Risk Assessments

It's crucial to understand the persistent maturity gap in Third-Party Risk Management. By examining each of the ten key findings uncovered in the State of Third-Party Risk Assessments 2026, critical disconnects are revealed between organizations' confidence in their third-party risk assessments, and the actual outcomes they achieve. When reviewing the findings and supporting data, consider how they reflect, or challenge, an organization's current approach, and use these insights to inform more effective third-party risk strategies in practice.

KEY FINDING 1

66% of large organizations believe their third-party assessments are effective at reducing breach risk, compared to only **40%** of small organizations

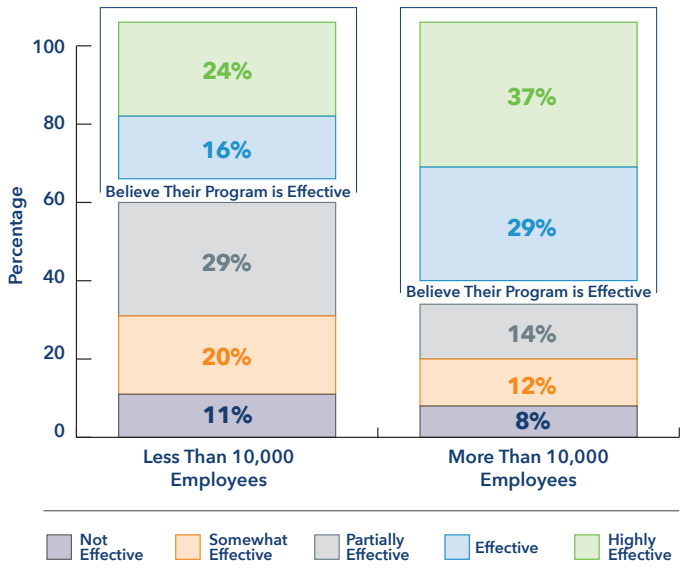
Confidence in TPRM Assessment Effectiveness Outpaces Intended Outcomes

Two-thirds of large organizations believe their third-party risk assessments are effective at reducing third-party breach risk, compared to just 40% of small organizations. This confidence gap highlights a core maturity disconnect, as belief in effectiveness does not consistently align with assessment speed, coverage, remediation, or breach outcomes.

What This Reveals About the Maturity Gap

This finding highlights a familiar experience for many organizations: confidence in third-party risk assessments themselves often grows faster than the programs. Formal processes, tooling, and governance can create a sense of control, even when day-to-day execution struggles to keep pace with scale and complexity. Over time, this gap between confidence and outcomes makes it harder for organizations to accurately assess their true risk posture, leaving them exposed to third-party-driven threats.

How effective are your organization's third-party risk assessments in reducing the likelihood of a third-party data breach?



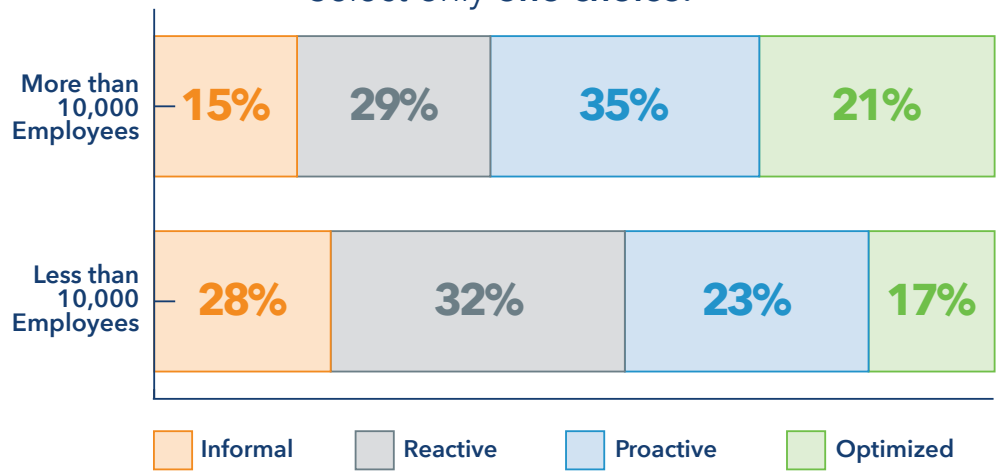
What the Data Shows

- **66% of large organizations** rate their TPRM assessments as effective, compared to 40% of small organizations, yet 89% of large organizations and 92% of small organizations experienced at least one third-party breach in the past year.
- **51% of respondents** reported they don't measure the effectiveness of their assessments at all, highlighting an indicator of limited understanding of true assessment effectiveness.
- While many organizations report high program effectiveness, they still experienced an average of **12 third-party breaches in the last year**, demonstrating that confidence does not correlate with reduced incident frequency.

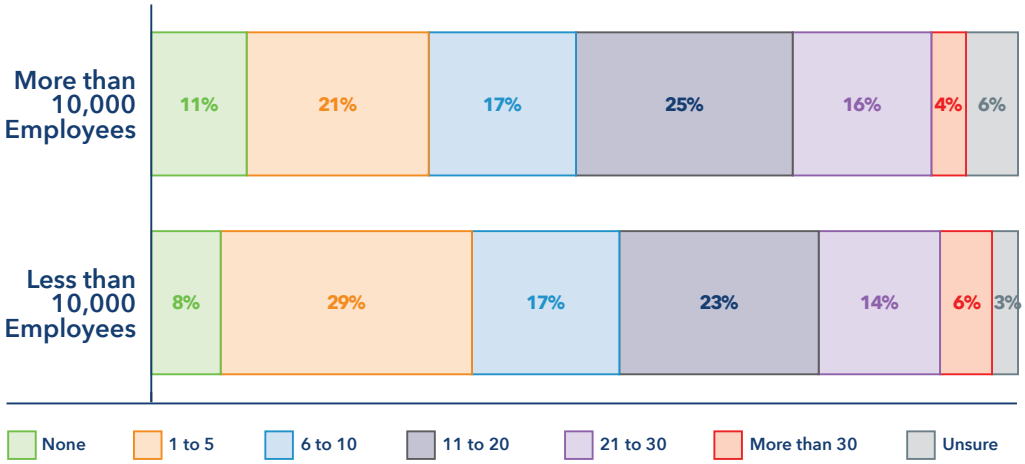
KEY FINDING 1 (CONT.)

66% of large organizations believe their third-party assessments are effective at reducing breach risk, compared to only **40%** of small organizations

How would you rate the maturity of your TPRM program? Select only **one choice.**



How many data breaches or security incidents caused by third parties did your organization experience over the past 12 months



KEY FINDING 2

Organizations average **one third-party breach per month**, with Financial Services organizations reporting the most third-party breaches

Third-Party Breaches are Frequent and Ongoing

Organizations report experiencing an average of 12 third-party breaches or security incidents in the last year, indicating that third-party risk is a recurring operational reality rather than an isolated event.

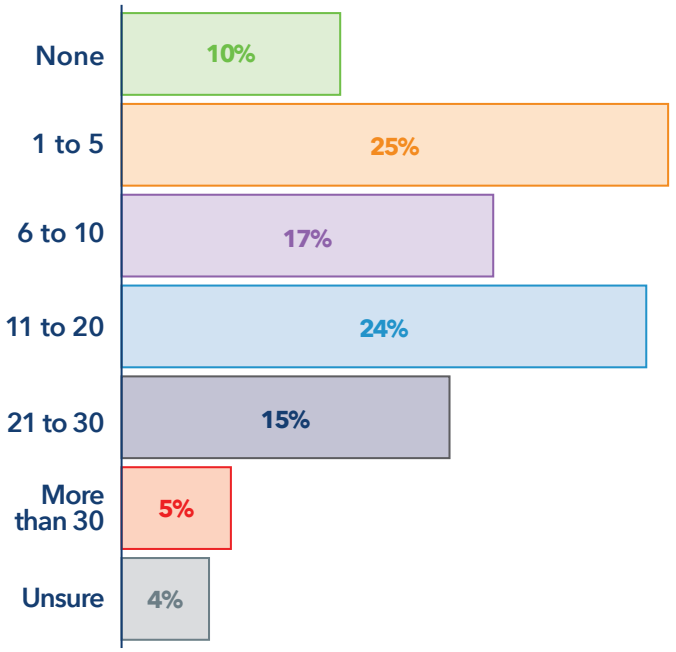
What This Reveals About the Maturity Gap

Frequent third-party breaches show that many organizations still react to incidents instead of preventing them. Even after teams complete assessments and document their third party's controls, risk continues to materialize across vendor relationships. This pattern suggests that existing programs are not yet translating process effort into sustained risk reduction.

What the Data Shows

- **90% of organizations** globally experienced at least one third-party breach in the past 12 months, with an average of 12 breaches per organization.
- **Breach occurrence is consistent across organization size** (89% of large organizations, 92% of small organizations) and across industries, indicating systemic exposure rather than isolated failure.

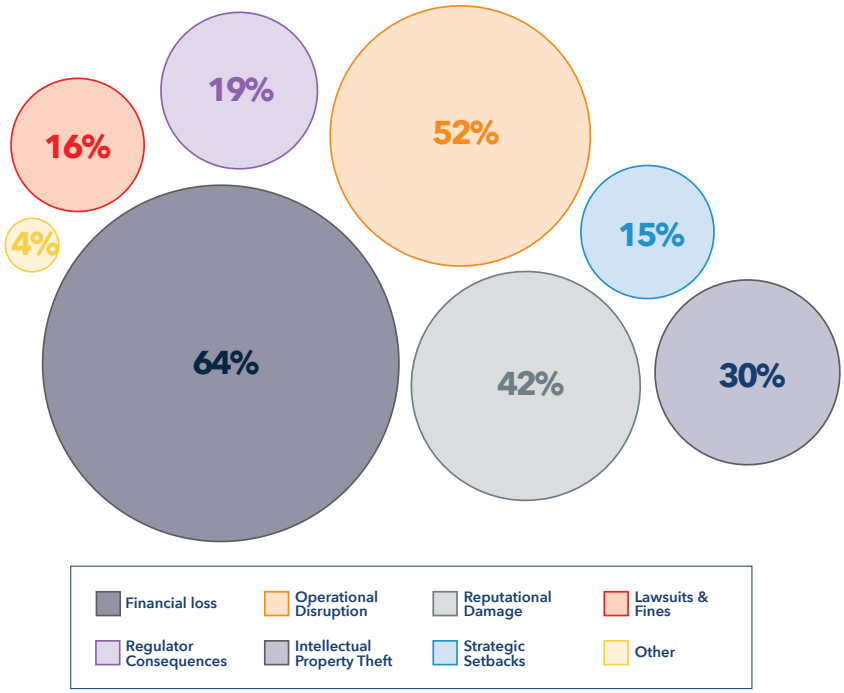
How many data breaches or security incidents caused by third parties did your organization experience over the past 12 months?



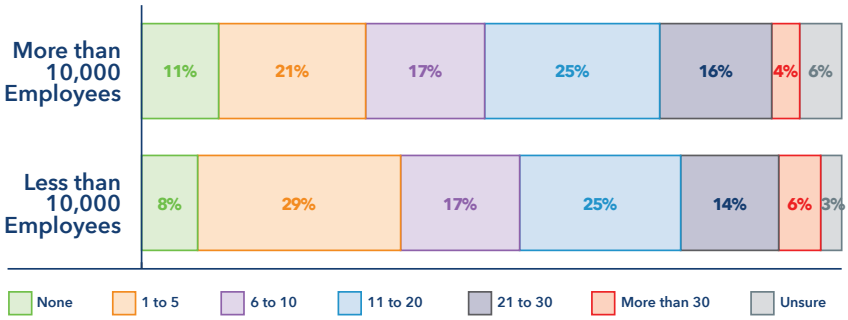
KEY FINDING 2 (CONT.)

Organizations average **one third-party breach per month**, with Financial Services organizations reporting the most third-party breaches

What were the consequences of the third-party data breach or security incident? Please select all that apply



How many data breaches or security incidents caused by third parties did your organization experience over the past 12 months?

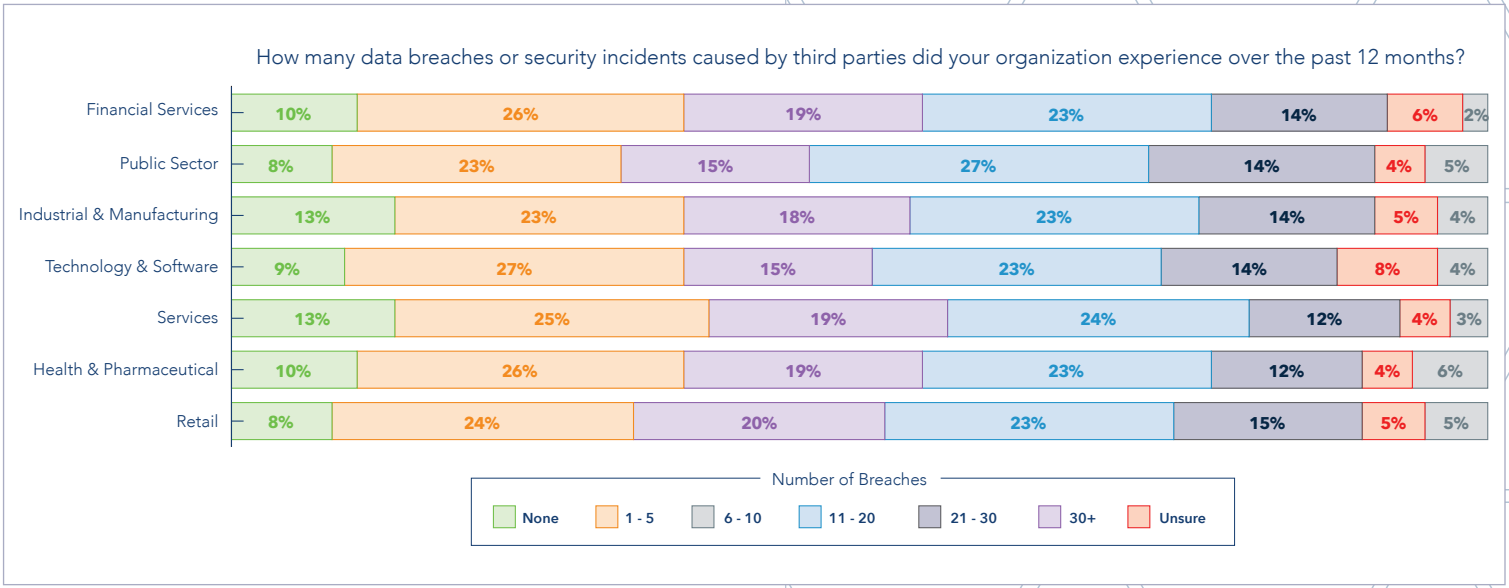


KEY FINDING 3

90% of Financial Services Organizations Experienced a Third-Party Breach in the Last Year

Financial Services Organizations Face Elevated Third-Party Risk

Nearly all Financial Services organizations report experiencing at least one third-party breach in the past year, despite heavy pressure to meet regulatory standards that require businesses to implement controls and processes to defend against breaches.



KEY FINDING 3 (CONT.)

90% of Financial Services Organizations Experienced a Third-Party Breach in the Last Year

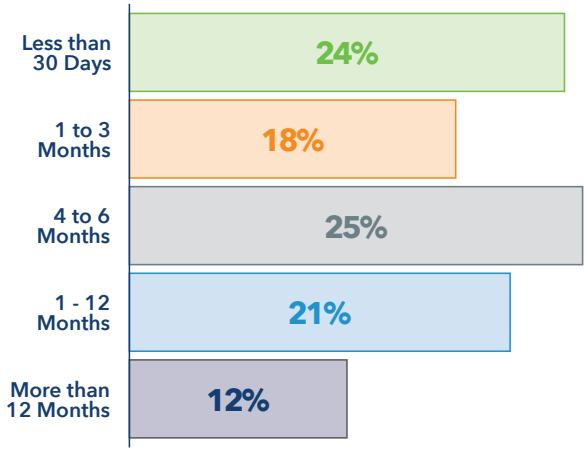
What This Reveals About the Maturity Gap

In highly regulated industries, strong governance and compliance requirements can create the appearance of maturity. However, persistent breach activity indicates that compliance-driven processes alone are not sufficient to manage complex third-party ecosystems. This gap highlights the limits of maturity defined primarily by regulatory alignment rather than operational effectiveness.

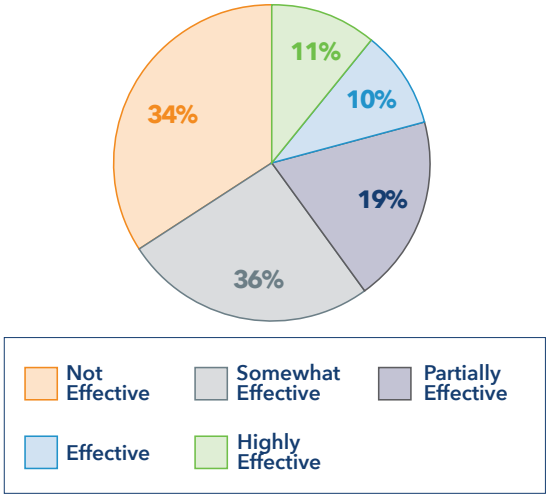
What the Data Shows

- In addition to high frequency of third-party breaches, **58% of Financial Services** organizations report third-party risk assessments take longer than four months, one of the longest assessment timelines across all industries surveyed.
- **60% of Financial Services** organizations rate their TPRM program as effective, despite 90% experiencing at least one third-party breach in the past year.

On average, how long does it take a financial services organization complete one third-party assessment (from launch to closure)



How effective are financial services orgs third-party risk assessments in reducing the likelihood of a third-party data breach?



KEY FINDING 4

64% of Large Organizations Report Assessments Take Longer Than **Four Months**

Assessment Timelines Are Too Slow to Keep Pace with Risk

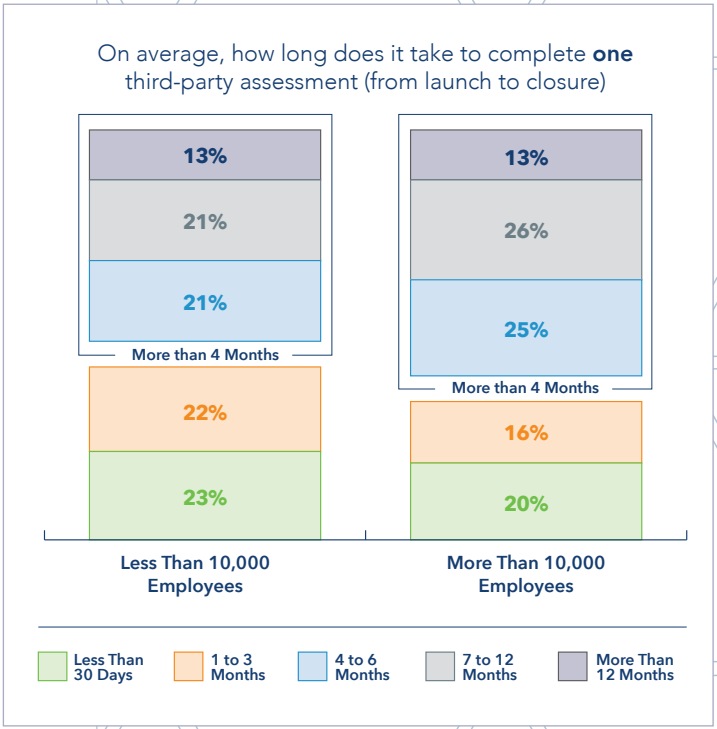
A majority of organizations report that third-party risk assessments take several months to complete, with large organizations especially likely to experience timelines exceeding four months (120+ days).

What This Reveals About the Maturity Gap

Extended assessment timelines create a structural delay between identifying risk and acting on it. When reviews take months to complete, organizations are often forced to onboard vendors before risk decisions are finalized. Over time, this lag undermines the effectiveness of assessment programs and increases exposure.

What the Data Shows

- **64% of large organizations** and 55% of small organizations report assessment timelines exceeding four months.
- **40% of organizations** report having an active assessment backlog, with 64% citing vendor non-responsiveness as a primary contributor.



KEY FINDING 4 (CONT.)

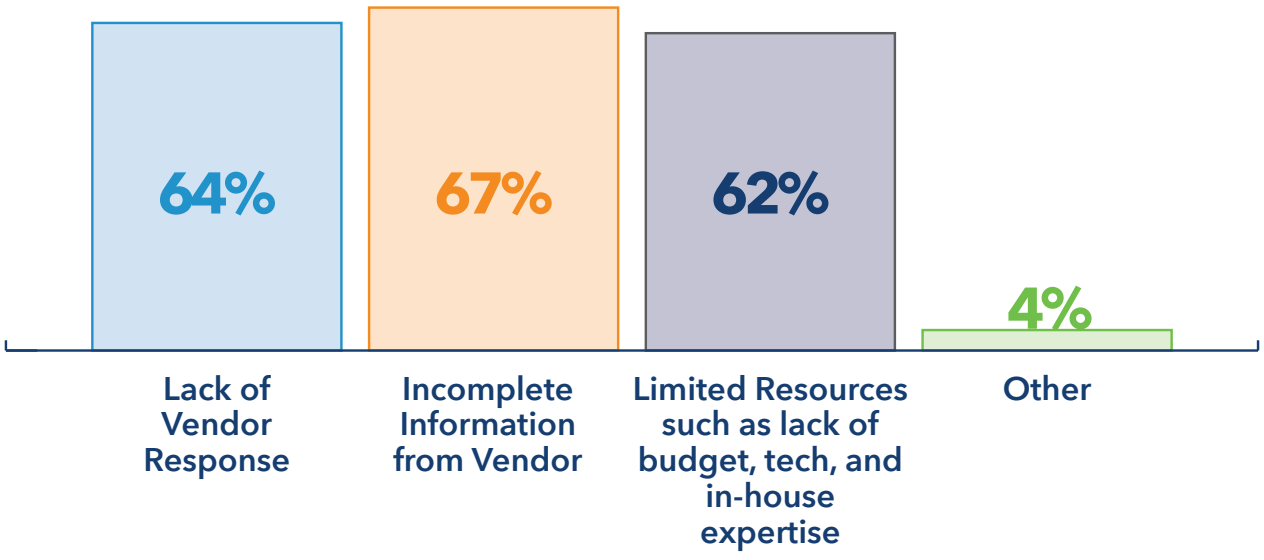
64% of Large Organizations Report Assessments Take Longer Than **Four Months**

KEY STAT

40%

of Companies Surveyed Have a Backlog of Third-Party Assessments.

What are the primary causes of backlogs in your assessment process? (Please select all that apply)



KEY FINDING 5

63% of Assessments Require More Than **40 Hours** of Team Effort

Third-Party Risk Assessments Currently Require Significant Internal Resources

Most organizations report that completing a single third-party risk assessment requires more than 40 personnel-hours across the team, limiting scalability for large vendor populations.

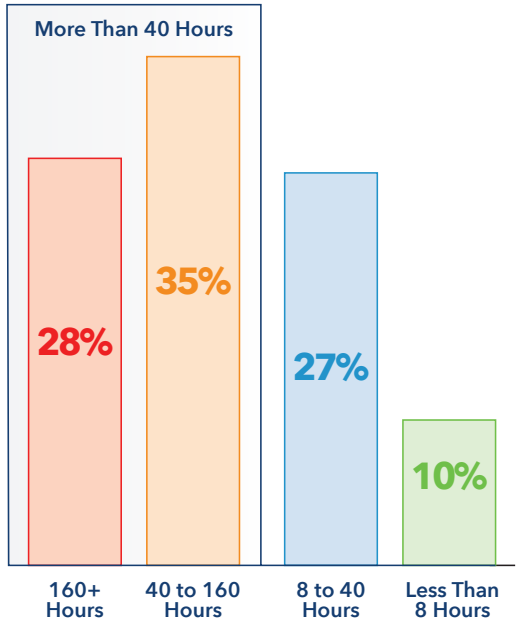
What This Reveals About the Maturity Gap

Heavy manual effort signals that many programs rely on individual contributors rather than scalable systems. As vendor volumes increase, this approach strains resources and slows execution. The result is a maturity gap where assessments exist but cannot keep up with demand.

What the Data Shows

- **63% of assessments** require more than 40 hours of team effort, including 28% that require more than 160 hours to complete.
- Effort levels are consistent across organization size; spreadsheets are utilized by **64% of large organizations and 63% of small organizations**.

On average, how many hours of your team's time does **one** third-party assessment take? (Select only one choice)



KEY STAT

28% Of the Companies Surveyed Reported Over **160 Team Hours to Complete One Assessment**

KEY FINDING 6

Two-Thirds of Organizations Still Utilize Spreadsheets in the Assessment Process

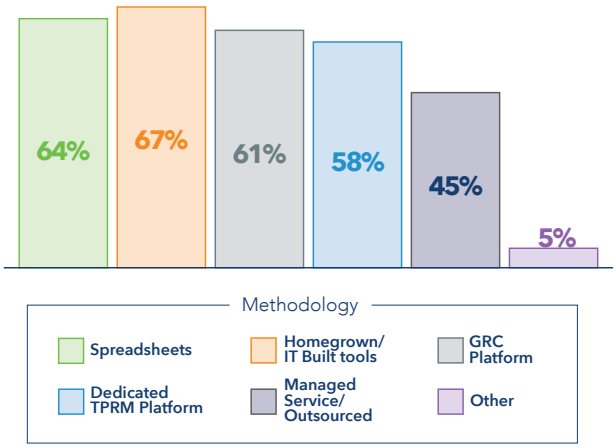
Manual Tools Remain Central to Assessment Execution

Despite increased availability of purpose-built platforms, spreadsheets and homegrown tools continue to play a role in how organizations conduct and manage third-party risk assessments, limiting the ability for teams to work at true efficiency.

What This Reveals About the Maturity Gap

Even partial reliance on spreadsheets reflects assessment programs that have formalized their processes but not modernized execution. Spreadsheet-based workflows are slow and error-prone, rely heavily on email for distribution and follow-up, and introduce version-control challenges that make reviews difficult to manage and analyze at scale. Without real-time visibility into whether third parties have started assessments or how complete responses are, teams lose control over timelines and progress.

What tools or platforms do you currently use to conduct third-party risk assessments? (Select all that apply)



What the Data Shows

- **64% of organizations** report using spreadsheets, and **67%** report using homegrown tools, indicating widespread tool fragmentation.
- **58% of organizations** report using a dedicated Third-Party Risk Management platform.
- **61% of organizations** report using a dedicated Governance, Risk, and Compliance (GRC) platform.

KEY STAT

ONLY 58% of the Companies Surveyed Utilize a Dedicated TPRM Platform in Their Third-Party Risk Program

KEY FINDING 7

60% of Organizations Wait Four Months or Longer for Vendor Responses to Assessments

Vendor Responsiveness Is a Major Roadblock for Effective Assessments

Delayed vendor responses and non-responses significantly extend assessment timelines, with many organizations reporting they wait months for questionnaire responses or receive no response at all from a meaningful portion of their vendor population.

What This Reveals About the Maturity Gap

Assessment timelines depend heavily on vendor responsiveness, so when organizations wait months to hear back from third parties, they lose control over their own risk processes. Delays and non-responses slow execution and force teams to make assumptions rather than data-based risk decisions. This dynamic limits the ability to manage third-party risk consistently at scale.

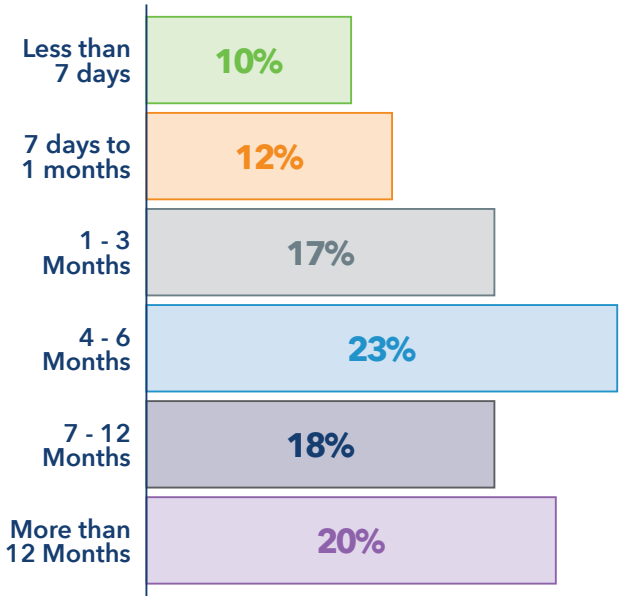
What the Data Shows

- Organizations surveyed reported that **27% of their vendors do not respond** at all to assessment requests.

KEY STAT

ON AVERAGE 27% of Third-Parties Never Respond to an Assessment

How long do vendors typically take to respond to your questionnaires? Please select one choice only.



KEY FINDING 8

Organizations Assess **Only 36%** of Their Third-Party Population, on Average

Assessment Coverage Remains Limited

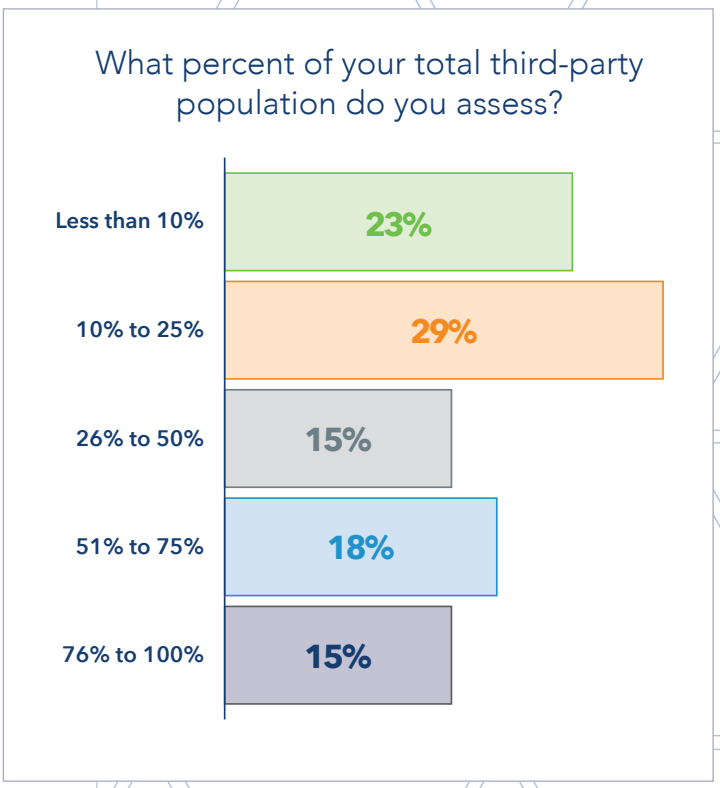
On average, organizations assess roughly one-third of their total third-party population, leaving large portions of vendor ecosystems outside formal risk assessment processes.

What This Reveals About the Maturity Gap

Assessing only a portion of an organization's large vendor population creates structural blind spots that are often the result of necessary prioritization. Faced with limited resources, organizations tend to focus assessments on vendors deemed highest risk, leaving mid- and lower-risk relationships largely unassessed. While this approach may be practical in the short term, and give the appearance that programs are effective, it allows risk in less-scrutinized vendors to go unchecked, creating gaps in coverage that undermine confidence in the program's overall effectiveness.

What the Data Shows

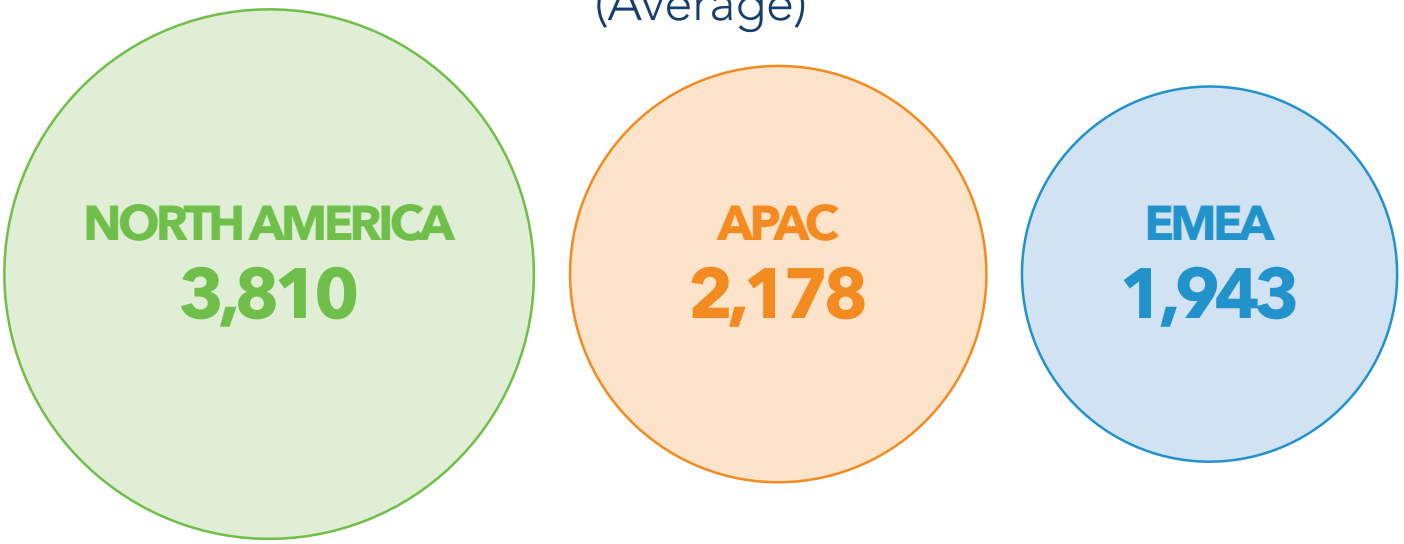
- The gap between intended and actual coverage persists across both large and small organizations, indicating the execution issue happens with third-party portfolios of all sizes.
- **Only 15% of organizations** report assessing 76–100% of vendors.



KEY FINDING 8 (CONT.)

Organizations Assess **Only 36%** of Their Third-Party Population, on Average

How many third parties are in your portfolio? (Average)



KEY STAT

ONLY 15% of Global Companies Assess 76 to 100 Percent of Their Vendors

KEY STAT

951 VENDORS is the Average Number of Vendors Assessed in an Ecosystem

KEY FINDING 9

Only **16%** of Organizations Complete **90–100% of Remediation** Before Onboarding

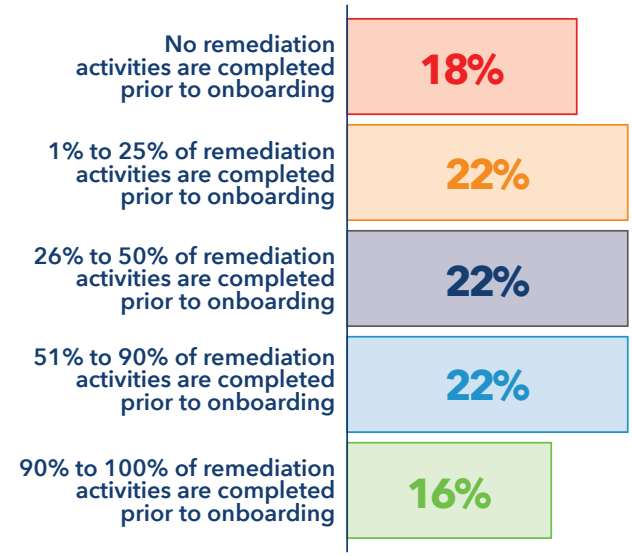
Organizations Prioritize Onboarding Speed Without Completing Remediation, Introducing Risk to Their Business

Only a small percentage of organizations complete most remediation activities before onboarding vendors, resulting in vendors with potentially unresolved control gaps being accepted into their environment.

What This Reveals About the Maturity Gap

When remediation is deferred, known risks are effectively accepted into the environment by default. In many cases, vendors are onboarded and contracts are finalized before remediation is complete, making it impractical to introduce new controls, SLAs, or contractual protections after the fact. Once the agreement is signed and the relationship is active, organizations have limited leverage to enforce remediation. Over time, these unresolved issues accumulate, reinforcing the gap between identifying risk and reducing it.

On average, what percentage of remediation activities are completed prior to onboarding?



What the Data Shows

- **18% of organizations** report not completing *any* remediation activities before onboarding vendors.
- **66% of organizations** cite resource constraints, and 46% cite immediate business need for the vendor as reasons remediation is deferred.

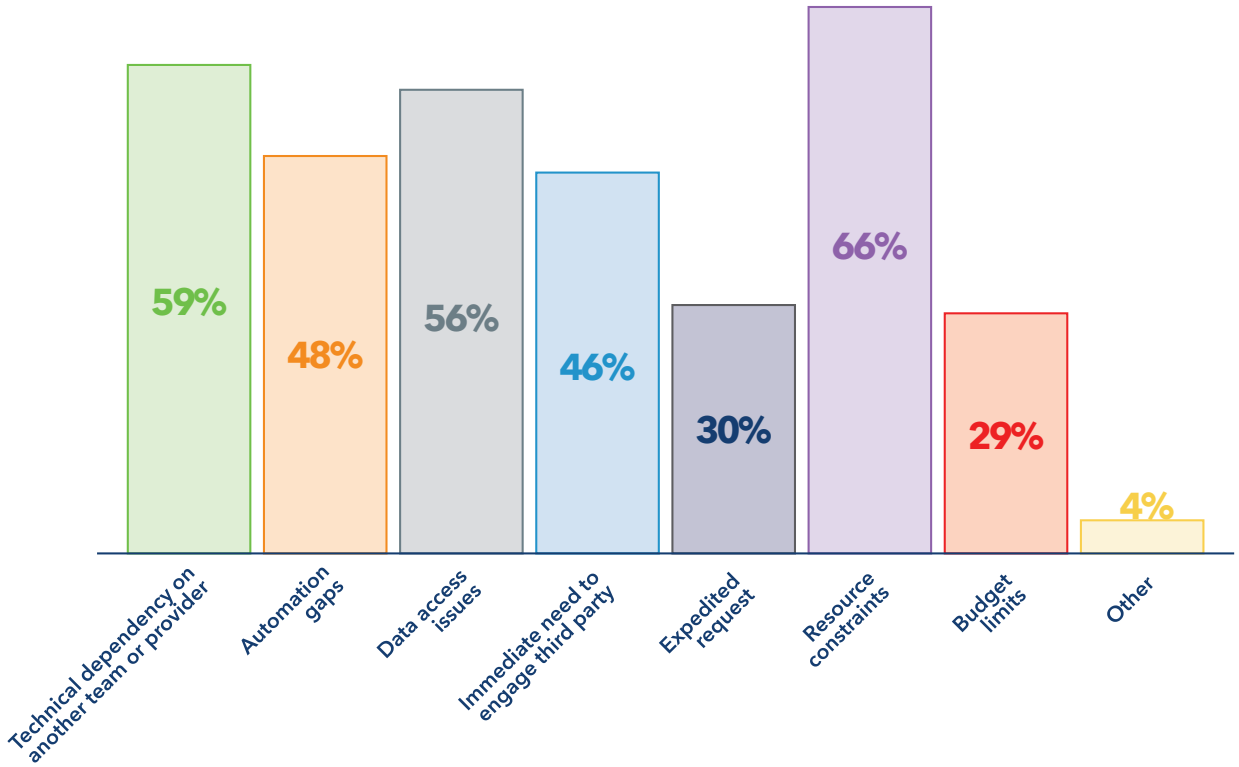
KEY FINDING 9 (CONT.)

Only **16%** of Organizations Complete **90–100% of Remediation** Before Onboarding

KEY STAT

66% of Companies Surveyed Do Not Complete Remediation before Onboarding due to Resource Constraints

If only 50 percent or less of remediation activities are completed, what were the reasons that prevented the completion of remediation before onboarding? (Select all that apply)



KEY FINDING 10

Fewer Than **One-Third** of Organizations Assess Fourth-Party Risk

Key Finding: Fourth-Party Risk Remains Largely Unaddressed by All Organizations

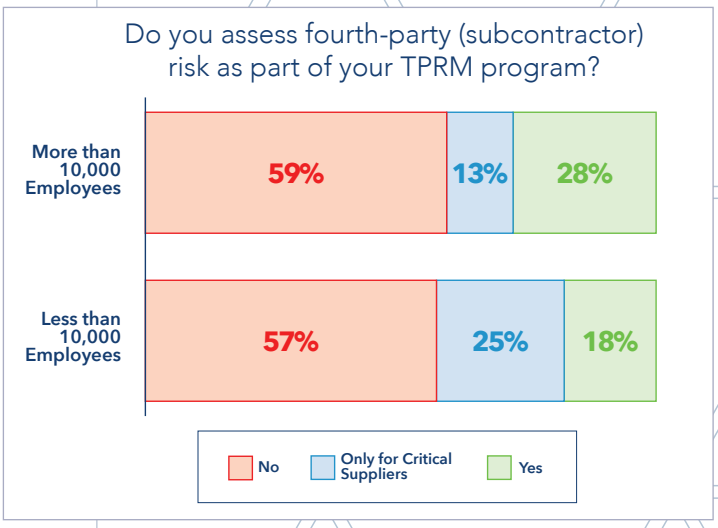
Most organizations do not assess fourth-party risk, and confidence in visibility beyond direct vendors drops sharply once risk extends into subcontractor and downstream relationships.

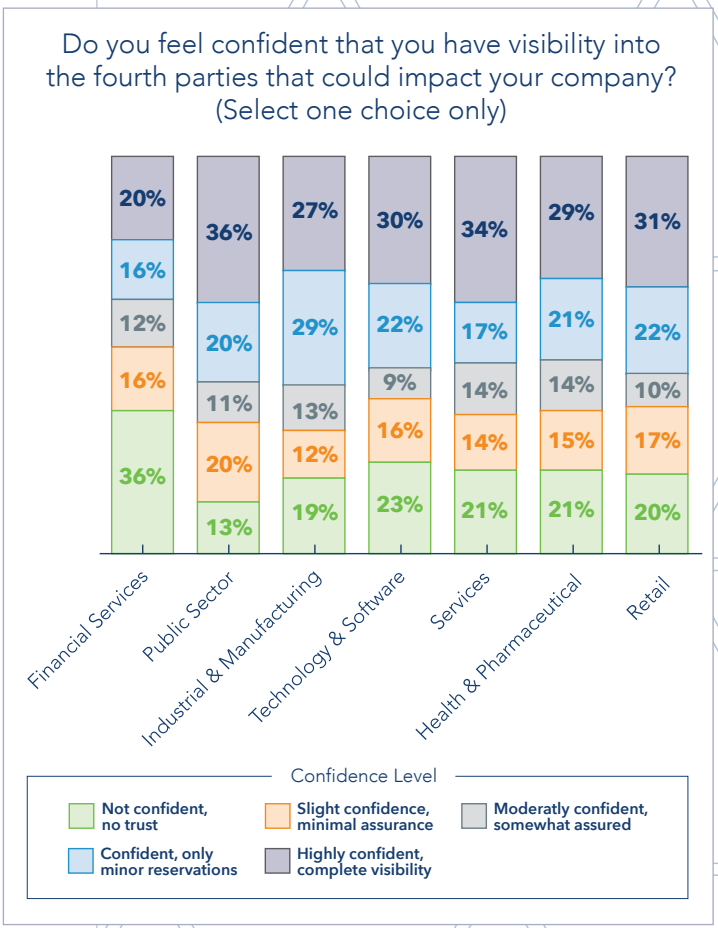
What This Reveals About the Maturity Gap

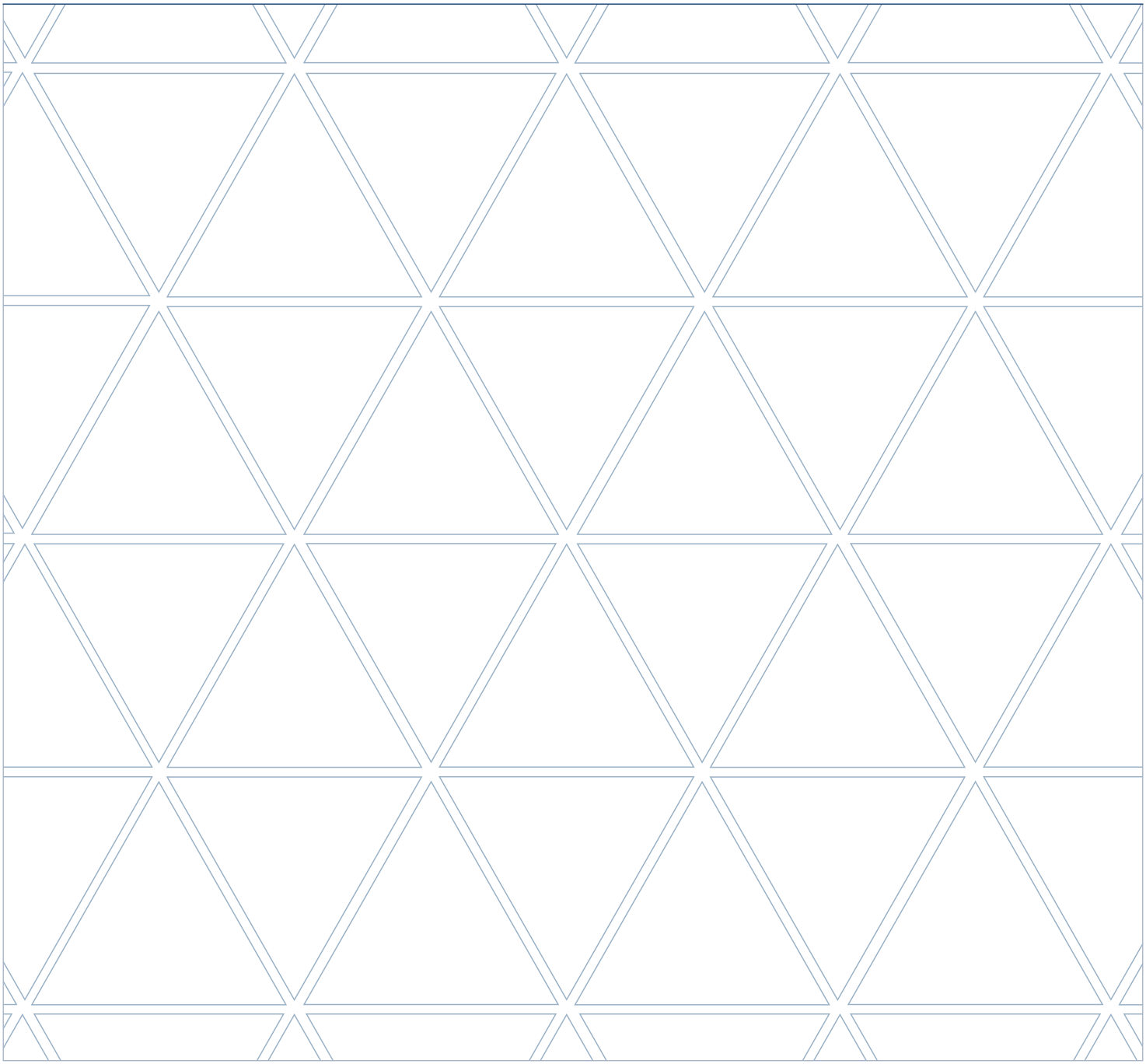
Fourth-party risk management is challenging, time-consuming, and oftentimes too much for teams to manage with their current processes. Limited attention to fourth-party risk shows how quickly visibility drops beyond direct vendors. As ecosystems become more interconnected, this lack of insight increases the likelihood of cascading incidents. The maturity gap widens when programs leave their extended ecosystem unmonitored.

What the Data Shows

- **Only 23% of organizations** assess fourth-party risk consistently, while 58% do not assess fourth-party risk at all.
- **38% of organizations** report no confidence or slight confidence in their visibility into fourth-party risk.







PART 3

Additional Survey Insights

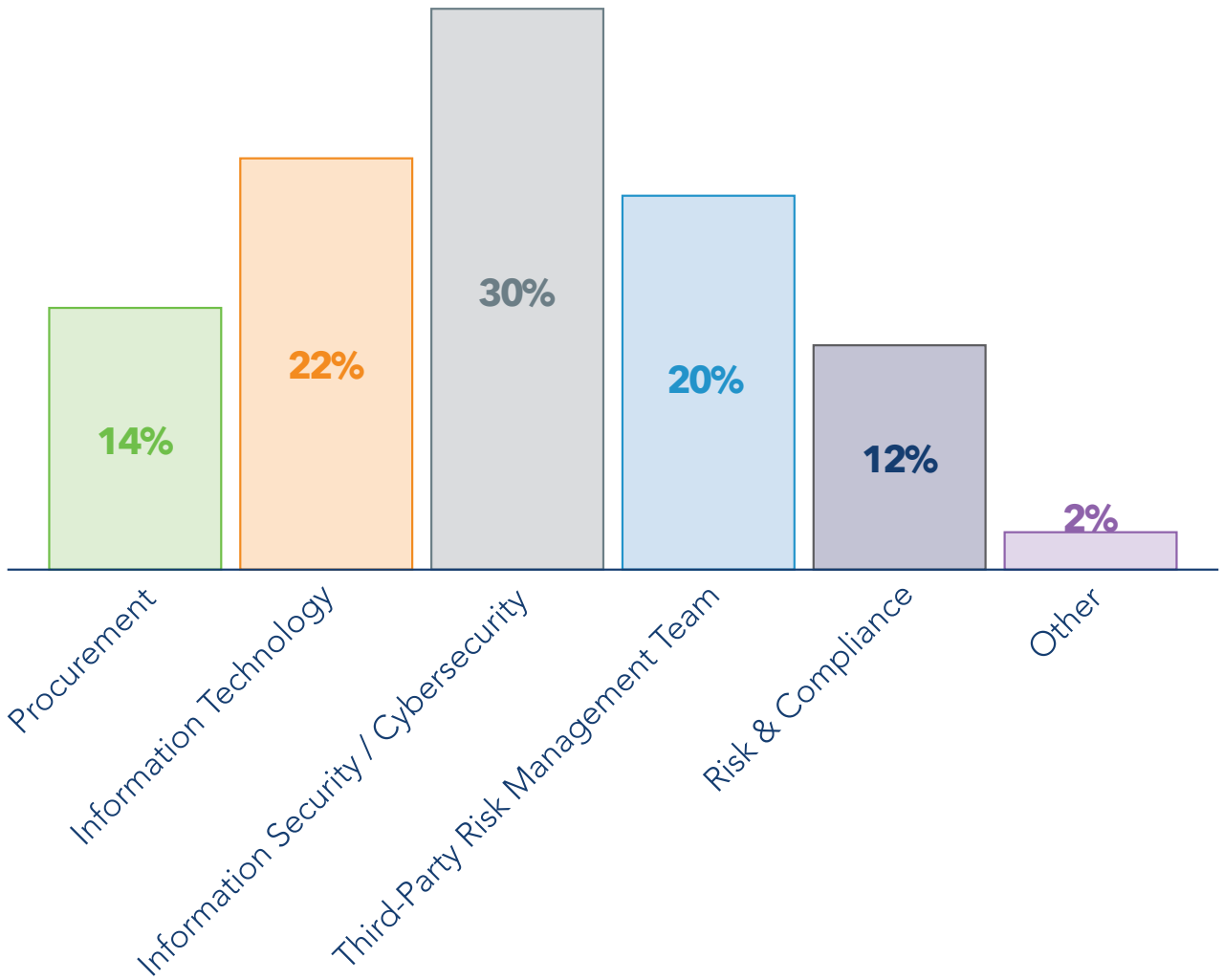
Beyond the headline findings, the survey revealed a deeper set of signals that further illustrate the day-to-day realities facing third-party risk teams. These additional insights surface how assessment programs are staffed, funded, and operated in practice, and where operational complexity, resource constraints, and emerging risks continue to challenge even well-established TPRM efforts.

Program Ownership, Staffing, and Accountability

Survey results show that responsibility for third-party risk assessments is distributed across multiple functions, often without clear ownership.

- InfoSec or cybersecurity teams most commonly own third-party risk assessments (30%), followed by information technology (22%), and TPRM team (20%)
- Only 49% of organizations measure the effectiveness of their third-party risk assessment program
- Large organizations are significantly more likely than small organizations to measure program effectiveness (61% vs. 38%)
- About one-fifth of organizations do not track remediation completion or escalation effectiveness as a measure of program success

Which function is most responsible for third-party risk assessments in your organization? (Please select one choice only)

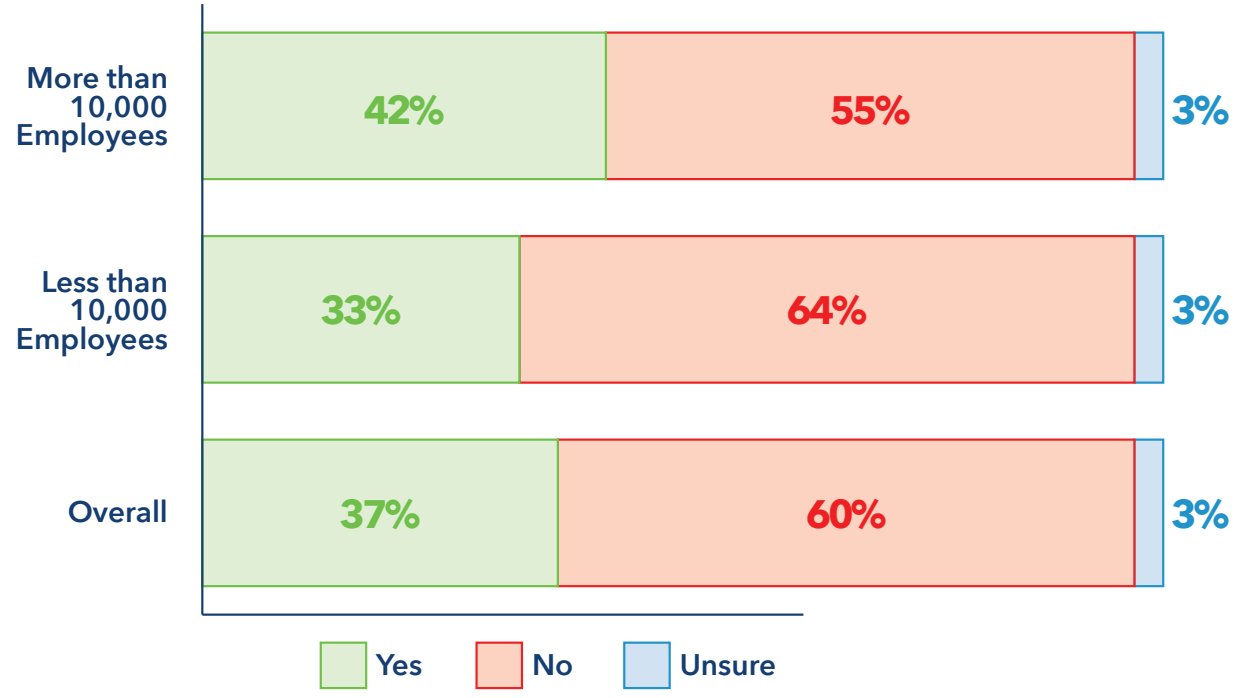


Budget, Investment, and Resource Allocation

Investment in third-party risk assessments remains inconsistent and is often misaligned with program scope.

- Only 37% of organizations report having a dedicated budget for third-party risk assessments
- Large organizations are more likely than small organizations to allocate a dedicated TPRM budget (42% vs. 33%)
- Among organizations with a dedicated budget, two-thirds reported spending $500,000 or more annually on Third-Party Risk Management

Does your organization budget allocate funds to support its third-party cybersecurity risk assessment program?

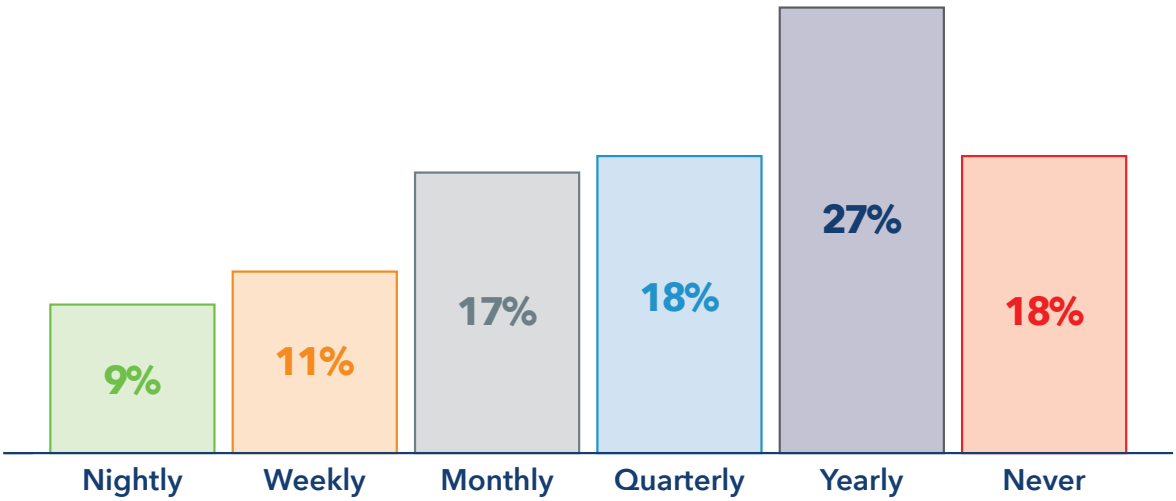


Assessment Cadence and Monitoring Practices

Assessment frequency and monitoring practices vary widely, limiting ongoing visibility into vendor and fourth-party risk.

- 58% of organizations do not assess fourth-party risk
- About a third of respondents expressed minimal confidence in their visibility into fourth parties that could impact their organization
- 27% of organizations only receive annual updates on their vendor's risk posture (continuous monitoring)
- 18% of organizations do not utilize continuous monitoring to supplement point-in-time assessments

How often do you receive updates on changes in vendor risk posture (continuous monitoring)? Please select one choice only.

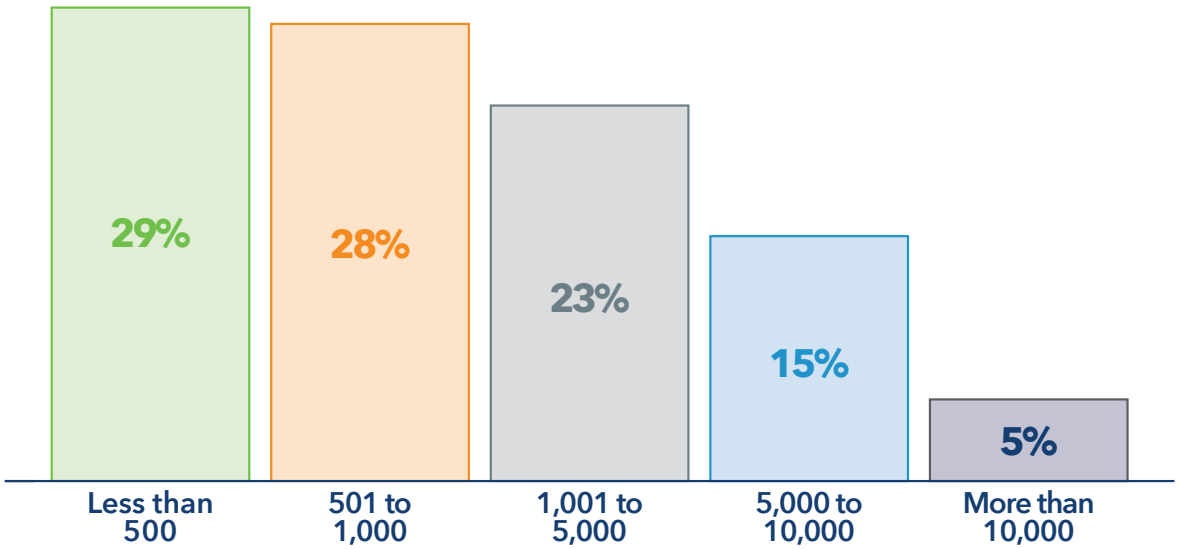


Vendor Population Characteristics and Concentration Risk

Organizations manage increasingly large and complex vendor ecosystems, often with limited prioritization.

- **61%** of organizations assess more than 660 third parties annually
- **33%** of organizations assess more than 1,300 third parties per year
- Enhanced due diligence is most often applied only to a subset of vendors, typically based on perceived criticality

How many third parties are in your portfolio?

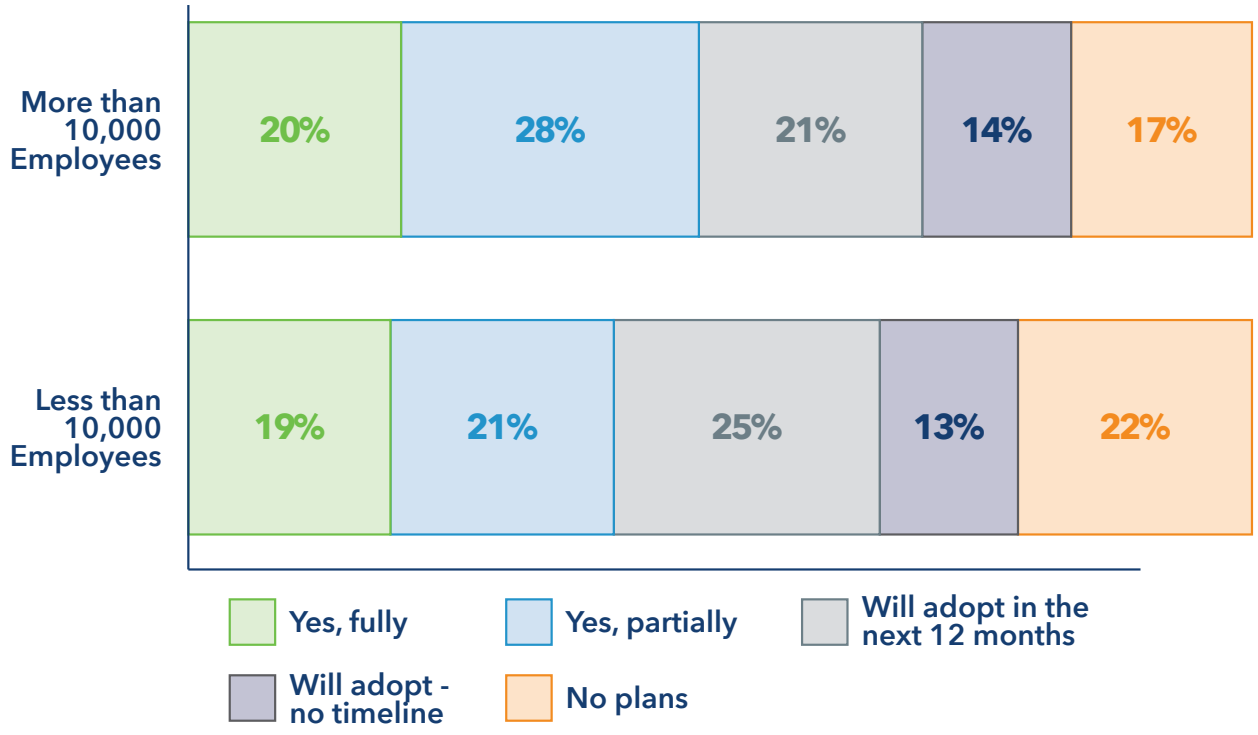


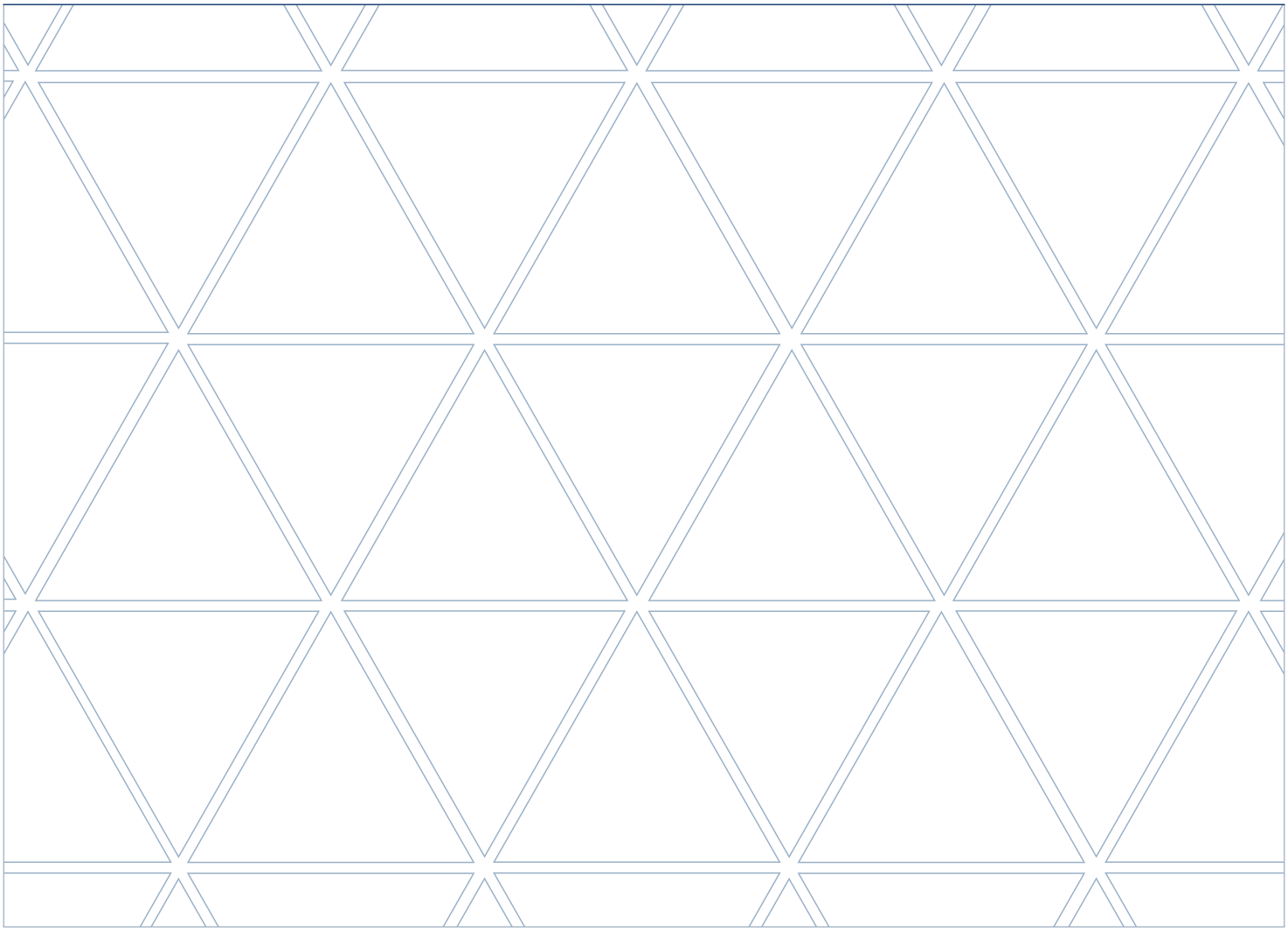
AI Adoption in Third-Party Risk Assessments

AI adoption in Third-Party Risk Management is growing, but most organizations remain in early or exploratory stages.

- 44% of organizations currently use AI to support third-party risk assessments (19% fully adopted, 25% partially adopted)
- An additional 37% plan to adopt AI within the next 12 months or have plans without a defined timeline
- AI adoption is slightly higher among large organizations (48%) than small organizations (40%)
- The most common reported benefits of AI include freeing staff for higher-value work (53%), real-time intelligence (48%), and better management (42%)

Has your organization adopted AI tools as part of its third-party risk management program? Please select one choice only





PART 4

Implications for Third-Party Risk Leaders

The findings in this report point to a clear conclusion: most organizations have invested in third-party risk assessment processes, but far fewer have invested in the capabilities required to operate those processes effectively at scale. The maturity gap identified throughout this research is not the result of a lack of effort or intent, but the result of teams being asked to do more with tools that were not designed for today's complex third-party ecosystems.

For third-party risk leaders, the implications of this report do not require starting over, but instead refocusing investment and attention on the areas that most directly influence outcomes.

Reframing the Role of Automation in TPRM Programs

Manual effort remains a defining characteristic of most present-day assessment programs. Long timelines, concentrated workloads, and incomplete coverage are all symptoms of processes that depend too heavily on human intervention. Automation, when applied intentionally, offers an opportunity to reduce friction without sacrificing rigor.

Rather than automating entire assessments end-to-end, organizations should focus automation on the points of greatest constraint: questionnaire distribution and collection, response validation, evidence handling, and issue tracking. Automating these steps reduces cycle times, frees subject-matter experts to focus on judgment-based decisions, and allows programs to scale without proportionally increasing headcount. Automation also gives third-party assurance teams the tools and capabilities they need to respond faster and accurately to assessments.

Improving Access to Risk Data = Better Decision Making

Vendor decisions often rely on fragmented, delayed, or incomplete risk information. Assessment results may exist, but procurement, security, legal, and business stakeholders cannot always access the results in a timely or usable form. Survey findings reinforce this pattern, showing persistent gaps between available risk data and the moments when teams need it most.

Improving data access does not require more reporting, but better tools and integration. When assessment data, remediation status, and risk ratings are accessible within existing workflows, organizations are better positioned to make informed decisions without slowing the business. Programs that prioritize timely access to reliable data are more likely to move from process completion to outcome-driven risk management.

Improving data access does not require more reporting, but better tools and integration

Shifting How Effectiveness Is Measured

Many organizations continue to measure success based on activity: the number of assessments completed, questionnaires sent, or policies enforced. While these metrics are useful, they do not capture whether risk is actually being reduced.

TPRM leaders should broaden how they define effectiveness. Metrics such as assessment cycle time, portfolio coverage, remediation completion, and reduction in repeat findings provide a clearer signal of program maturity. Over time, these measures help organizations identify where automation, tooling, or process changes will have the greatest impact.

Closing the Maturity Gap

The good news is that the maturity gap highlighted throughout this research is not insurmountable. Organizations that invest in scalable automation, prioritize access to actionable risk data, and measure success through outcomes rather than activity are better positioned to manage third-party risk as ecosystems continue to grow.

As third-party relationships become more interconnected and risk exposure extends beyond direct vendors, the ability to operate assessment programs efficiently and intelligently will become a defining characteristic of mature TPRM programs. The data in this report provides a benchmark for where organizations stand today, and a roadmap for where they can focus next.

The ability to operate assessment programs efficiently and intelligently will become a defining characteristic of mature TPRM programs

Continue to the Appendix to review the full survey methodology, complete question set, and detailed raw response data that informed this report.

ProcessUnity

ABOUT PROCESSUNITY

ProcessUnity is *the* Third-Party Risk Management (TPRM) company. Our software platforms and data services protect customers from cybersecurity threats, breaches, and outages that originate from their ever-growing ecosystem of business partners. By combining the world's largest third-party risk data exchange, the leading TPRM workflow platform, and powerful artificial intelligence, ProcessUnity extends third-party risk, procurement, and cybersecurity teams so they can cover their entire vendor portfolio. With ProcessUnity, organizations of all sizes reduce assessment work while improving quality, securing intellectual property and customer data so business operations continue to operate uninterrupted.

See how at www.processunity.com.

ADDRESS
ProcessUnity
33 Bradford Street
Concord, MA 01742
United States

SOCIALS
Twitter: @processunity
LinkedIn: processunity

WEBSITE
www.processunity.com

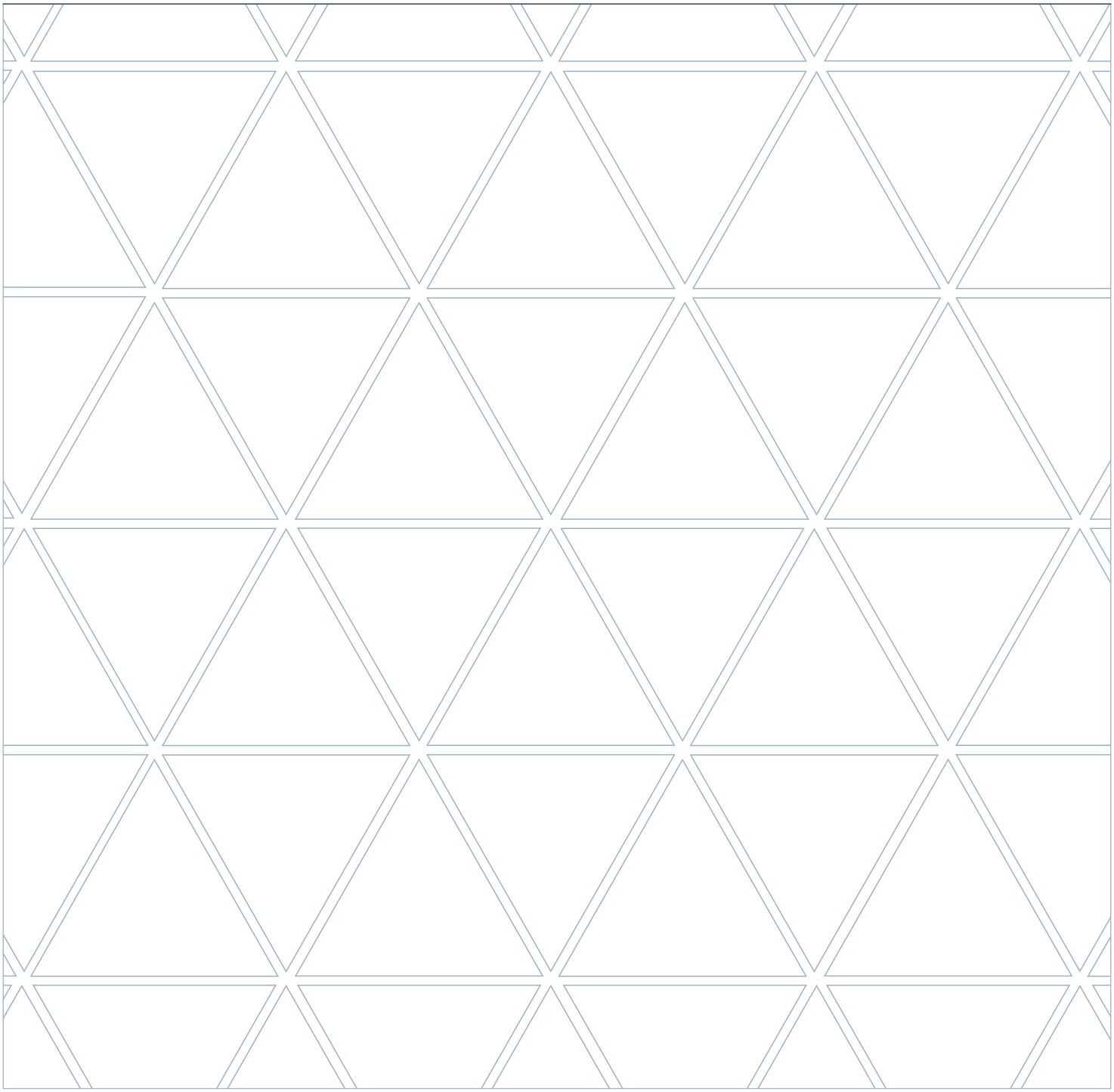
EMAIL
info@processunity.com

Speak with ProcessUnity

Ponemon INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.



DATA SET

Appendix

APPENDIX 1: LOCATION

Data Tables

2026 Survey Responses

Survey Responses	North America	APAC	EMEA	GLOBAL
Sampling Frame	18,505	13,290	13,880	45,675
Total Returns	721	465	501	1,687
Rejected or Screened Surveys	89	63	70	222
Overall sample	**632**	**402**	**431**	**1,465**

S1. Does your organization have a Third-Party Risk Management program that involves conducting third-party risk assessments?	North America	APAC	EMEA	GLOBAL
Yes	63%	57%	58%	59%
No	37%	43%	42%	41%
Total	**100%**	**100%**	**100%**	**100%**

S2. How involved are you in your organization's approach to assessing data risks created through outsourcing business functions to third parties?	North America	APAC	EMEA	GLOBAL
Very involved	40%	36%	41%	39%
Involved	42%	42%	38%	41%
Moderately involved	18%	22%	21%	20%
Not involved	0%	0%	0%	0%
Total	**100%**	**100%**	**100%**	**100%**

Part 1. Background on your Portfolio

Q1: How many third parties are in your portfolio?	North America	APAC	EMEA	GLOBAL
Less than 500	18%	34%	36%	29%
501 to 1,000	20%	31%	33%	28%
1,001 to 5,000	32%	20%	18%	23%
5,001 to 10,000	21%	12%	11%	15%
More than 10,000	9%	3%	2%	5%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated Average	**3,810**	**2,178**	**1,943**	**2,643**

Q2. What percent of your total third-party population **should you** assess? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Less than 10 percent	20%	23%	25%	23%
10 percent to 25 percent	23%	27%	25%	25%
26 percent to 50 percent	16%	23%	19%	19%
51 percent to 75 percent	17%	12%	14%	14%
76 percent to 100 percent	24%	15%	17%	19%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated Average	**43%**	**35%**	**37%**	**38%**

Q3. What percent of your total third-party population **do you** assess? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Less than 10 percent	20%	24%	26%	23%
10 percent to 25 percent	33%	28%	26%	29%
26 percent to 50 percent	16%	14%	16%	15%
51 percent to 75 percent	17%	16%	20%	18%
76 percent to 100 percent	14%	18%	12%	15%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated Average	**36%**	**37%**	**35%**	**36%**

Q4. How do you determine if a vendor requires a third-party risk assessment? Please select all that apply.	North America	APAC	EMEA	GLOBAL
The third party is critical to our organization's ability to meet its business objectives and obligations	65%	68%	71%	68%
The third party has access to our most confidential information such as trade secrets and intellectual property	68%	68%	68%	68%
The third party has the potential to affect our organization's ability to comply with regulations	70%	67%	69%	69%
Other	5%	4%	3%	4%

Q5. Do you have an inherent risk process that determines the frequency of third-party risk assessments?	North America	APAC	EMEA	GLOBAL
Yes	58%	48%	51%	52%
No	42%	52%	49%	48%
Total	**100%**	**100%**	**100%**	**100%**

Q6. If yes, do you scope your assessment questionnaire or employ a specific questionnaire based on the third-party's inherent risk?	North America	APAC	EMEA	GLOBAL
Yes	48%	56%	54%	53%
No	52%	44%	46%	47%
Total	**100%**	**100%**	**100%**	**100%**

Q7. Which risk domains or functions are included in your third-party risk assessments? Please select all that apply.	North America	APAC	EMEA	GLOBAL
Financial	59%	49%	62%	57%
IT Security/cybersecurity	69%	51%	54%	58%
Artificial Intelligence	26%	12%	17%	18%
Compliance/regulations	50%	46%	62%	53%
Operations	60%	59%	57%	59%
Geographic locations	33%	29%	25%	29%
Environmental, Social and Governance (ESG)	18%	9%	26%	18%
Other	5%	6%	5%	5%

Part 2. Operating Model and Methods

Q8. How would you rate the maturity of your TPRM program? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Ad hoc or informal: There are only a few defined processes in place for third-party assessments	23%	20%	22%	22%
Reactive: Assessments are defined for key third parties but they are still manual and inconsistent	28%	32%	31%	30%
Proactive: Assessments are standardized and repeatable for most third parties with defined policies, tools, and remediation processes	29%	30%	28%	29%
Optimized: The TPRM program is fully embedded in business operations using automation, advanced analytics, and continuous monitoring to manage vendor risk proactively	20%	18%	19%	19%
Total	**100%**	**100%**	**100%**	**100%**

Q9. What type of questionnaire do you use to assess your third parties? Please select only one choice.	North America	APAC	EMEA	GLOBAL
We developed the questionnaire	30%	23%	23%	25%
We use an industry-standard questionnaire such as SIG, CAIQ	28%	26%	24%	26%
Compliance/regulations	19%	25%	26%	24%
We use a combination of our own questionnaire and an industry-standard questionnaire	23%	24%	26%	24%
Other	0%	2%	1%	1%
Total	**100%**	**100%**	**100%**	**100%**

Q10. What tools or platforms do you currently use to conduct third-party risk assessments? Please select all that apply.	North America	APAC	EMEA	GLOBAL
Spreadsheets	59%	63%	69%	64%
Homegrown/IT built tools	71%	63%	68%	67%
GRC Platform	63%	58%	61%	61%
Dedicated TPRM Platform	60%	59%	56%	58%
Managed Service/outsourced	44%	48%	44%	45%
Other	5%	4%	6%	5%

Q11. In addition to questionnaires, which data sources does your TPRM team use when assessing third parties?	North America	APAC	EMEA	GLOBAL
Vendor documentation of practices and policies	53%	45%	56%	51%
Independent ratings of the organization's cybersecurity and risk posture	48%	47%	39%	45%
Threat intelligence feeds	45%	50%	47%	47%
Financial statements and reports	27%	26%	30%	28%
Regulatory reports or publicly available compliance data	34%	32%	27%	31%
Service Level Agreements (SLA)	67%	63%	57%	62%
Environmental, Social, and Governance (ESG)	18%	16%	13%	16%
Other	2%	3%	2%	2%

Q12. Do you assess fourth-party (subcontractor) risk as part of your TPRM program?	North America	APAC	EMEA	GLOBAL
Yes	26%	19%	23%	23%
Only for critical suppliers	18%	24%	17%	19%
No	56%	57%	60%	58%
Total	**100%**	**100%**	**100%**	**100%**

Q13. Do you feel confident that you have visibility into the fourth parties that could impact your company? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Not confident, no trust	26%	22%	19%	22%
Slight confidence, minimal assurance with significant doubts	12%	16%	20%	16%
Moderately confident, somewhat assured	10%	12%	11%	11%
Confident, only minor reservations	23%	18%	19%	20%
Highly confident, complete trust in visibility	29%	32%	31%	31%
Total	**100%**	**100%**	**100%**	**100%**

Part 3. Processes and Performance

Q14. On average, how long does it take to complete one third-party assessment (from launch to closure)?	North America	APAC	EMEA	GLOBAL
Less than 30 days	21%	23%	20%	21%
1 to 3 months	18%	22%	17%	19%
4 to 6 months	23%	21%	25%	23%
7 to 12 months	27%	21%	23%	24%
More than 12 months	11%	13%	15%	13%
Total	**100%**	**100%**	**100%**	**100%**

Q15. On average, how many hours of your team's time does one third-party assessment take? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Less than 8 hours (1 day)	11%	10%	8%	10%
8 to 40 hours (1 week)	29%	26%	27%	27%
41 to 160 hours (1 month)	32%	38%	34%	35%
More than 160 hours	28%	26%	31%	28%
Total	**100%**	**100%**	**100%**	**100%**

Q16. How long do vendors typically take to respond to your questionnaires? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Less than 7 days	9%	12%	8%	10%
7 days to 1 month	13%	11%	12%	12%
1 to 3 months	19%	17%	15%	17%
4 to 6 months	24%	20%	26%	23%
7 to 12 months	18%	19%	16%	17%
More than 12 months	17%	21%	23%	20%
Total	**100%**	**100%**	**100%**	**100%**

Q17a. Do you currently have a backlog of third-party assessments?	North America	APAC	EMEA	GLOBAL
Yes	48%	41%	32%	40%
No	52%	59%	68%	60%
Total	**100%**	**100%**	**100%**	**100%**

Q17b. If yes, what are the primary causes of backlogs in your assessment process? Please select all that apply.	North America	APAC	EMEA	GLOBAL
Lack of vendor response	73%	58%	62%	64%
Incomplete information from vendor	68%	65%	68%	67%
Limited resources such as lack of budget, technology and in-house expertise	63%	53%	70%	62%
Other	3%	4%	5%	4%

Q18. What percentage of third-party responses require further attention or follow up with the third party? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Less than 10 percent	23%	21%	20%	21%
10 percent to 25 percent	17%	15%	19%	17%
26 percent to 50 percent	19%	22%	23%	22%
51 percent to 75 percent	20%	19%	18%	19%
76 percent to 100 percent	21%	23%	20%	21%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated average	**42%**	**44%**	**42%**	**43%**

Q19. How long does it typically take to remediate issues with one third party found during a third-party assessment? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Less than 7 days	11%	13%	9%	11%
7 days to 1 month	16%	16%	13%	15%
1 to 3 months	17%	20%	18%	18%
4 to 6 months	22%	13%	24%	20%
7 to 12 months	20%	12%	16%	16%
More than 12 months	14%	26%	20%	20%
Total	**100%**	**100**	**100%**	**100%**
Extrapolated average (months)	**5.4**	**5.9**	**6.0**	**5.8**

Part 4. Vendor Engagement and Risk Findings

Q20. Approximately what percentage of your third parties do not respond to your assessment questionnaires?	North America	APAC	EMEA	GLOBAL
None	3%	8%	11%	7%
Less than 5 percent	11%	12%	13%	12%
5 percent to 10 percent	16%	14%	19%	16%
11 percent to 25 percent	21%	19%	20%	20%
26 percent to 50 percent	23%	24%	17%	22%
More than 50 percent	26%	23%	20%	23%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated average	**30%**	**28%**	**24%**	**27%**

Q21. How often do you receive updates on changes in vendor risk posture (continous monitoring)? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Nightly	9%	7%	11%	9%
Weekly	12%	11%	10%	11%
Monthly	18%	17%	16%	17%
Quarterly	16%	20%	18%	18%
Yearly	29%	26%	26%	27%
Never	16%	19%	19%	18%
Total	**100%**	**100%**	**100%**	**100%**

Q22. Approximately what percentage of your third parties require remediation activities during the onboarding process to meet your security and privacy requirements?	North America	APAC	EMEA	GLOBAL
None	5%	6%	8%	6%
Less than 5 percent	13%	13%	12%	13%
5 percent to 10 percent	20%	17%	21%	19%
11 percent to 25 percent	17%	19%	16%	18%
26 percent to 50 percent	22%	23%	21%	22%
More than 50 percent	23%	22%	22%	22%
Total	**100%**	**100%**	**100%**	**100%**

Q23. On average, what percentage of remediation activities are completed prior to onboarding?	North America	APAC	EMEA	GLOBAL
No remediation activities are completed prior to onboarding	19%	16%	20%	18%
1 percent to 25 percent of the third parties that required remediation activities are completed	20%	21%	23%	22%
26 percent to 50 percent of the third parties that required remediation activities are completed	23%	24%	18%	22%
51 percent to 90 percent of the third parties that required remediation activities are completed	21%	26%	20%	22%
90 percent to 100 percent of the third parties that required remediation activities are completed	17%	13%	19%	16%
Total	**100%**	**100%**	**100%**	**100%**

Q24. If only 50 percent or less of remediation activities are completed, what were the reasons that prevented the completion of remediation before onboarding? Please select all that apply.	North America	APAC	EMEA	GLOBAL
Technical dependency on another team or provider	63%	59%	55%	59%
Automation gaps	49%	45%	51%	48%
Data access issues	56%	60%	53%	56%
Immediate need to engage third party	46%	49%	42%	46%
Expedited request (where risk is accepted)	28%	33%	30%	30%
Resource constraints (staff's time)	67%	61%	69%	66%
Budget limits	36%	27%	23%	29%
Other	3%	4%	5%	4%

Part 5. Governance and Team

Q25. Which function is most responsible for third-party risk assessments in your organization? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Procurement	12%	14%	17%	14%
Information Technology	21%	23%	20%	22%
Information Security / Cybersecurity	30%	27%	33%	30%
The Third-Party Risk Management team	23%	21%	16%	20%
Risk and Compliance	11%	12%	14%	12%
Other	3%	3%	0%	2%
Total	**100%**	**100%**	**100%**	**100%**

Q27. How many FTEs (full-time equivalents) are dedicated to vendor risk assessments in your organization?	North America	APAC	EMEA	GLOBAL
None	5%	9%	5%	6%
1 to 5	41%	39%	40%	40%
6 to 10	35%	33%	32%	33%
11 to 20	11%	13%	14%	13%
21 to 50	5%	4%	6%	5%
More than 50	3%	2%	3%	3%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated average	**9**	**8**	**10**	**9**

Q27a. Do you outsource any part of the assessment process (e.g., collection, validation, monitoring)?	North America	APAC	EMEA	GLOBAL
Yes	46%	44%	39%	43%
No	54%	56%	61%	57%
Total	**100%**	**100%**	**100%**	**100%**

Q27b. If yes, what part of the assessment process do you outsource? Please select all that apply.	North America	APAC	EMEA	GLOBAL
Collection	61%	57%	60%	59%
Validation	47%	43%	42%	44%
Monitoring	63%	55%	58%	59%
Other	4%	1%	0%	2%

Part 6. Outcomes, Maturity, and Budget

Q28. How effective are your organzation's third-party risk assessments in reducing the likelihood of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1=not effective to 10=highly effective.	North America	APAC	EMEA	GLOBAL
1 or 2	8%	12%	9%	10%
3 or 4	13%	11%	24%	16%
5 or 6	19%	23%	22%	21%
7 or 8	24%	23%	21%	23%
9 or 10	36%	31%	24%	30%
Total	**100%**	**100%**	**100%**	**100%**

Q29a. How many data breaches or security incidents caused by third parties did your organization experience over the past 12 months?	North America	APAC	EMEA	GLOBAL
None	10%	8%	12%	10%
1 to 5	21%	29%	25%	25%
6 to 10	18%	17%	16%	17%
11 to 20	25%	23%	25%	24%
21 to 30	16%	14%	13%	15%
More than 30	5%	6%	4%	5%
Unsure	5%	3%	5%	4%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated average	**12**	**12**	**11**	**12**

Q29b. If yes, what were the consequences of the third-party data breach or security incident? Please select all that apply.	North America	APAC	EMEA	GLOBAL
Financial loss	56%	48%	52%	52%
Operational disruptions	69%	63%	60%	64%
Reputational damage	35%	42%	41%	42%
Lawsuits and fines	16%	14%	18%	16%
Regulatory consequences	19%	21%	18%	19%
Intellectual property theft	31%	28%	32%	30%
Strategic setbacks	17%	14%	15%	15%
Other	3%	4%	5%	4%

Q30a. Did your third parties alert you to any security incidents generated by fourth parties in the last 12 months?	North America	APAC	EMEA	GLOBAL
Yes	46%	38%	39%	41%
No	54%	62%	61%	59%
Total	**100%**	**100%**	**100%**	**100%**

Q30b. If yes, how many alerts did you receive in the past 12 months?	North America	APAC	EMEA	GLOBAL
None	0%	0%	0%	0%
1 to 5	18%	19%	21%	19%
6 to 10	23%	21%	20%	21%
11 to 20	31%	29%	33%	31%
21 to 30	20%	24%	24%	23%
More than 30	8%	7%	2%	6%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated average	**15**	**16**	**14**	**15**

Q31a. Does your organization measure the effectiveness of your TPRM assessment program?	North America	APAC	EMEA	GLOBAL
Yes	61%	38%	49%	49%
No	39%	62%	51%	51%
Total	**100%**	**100%**	**100%**	**100%**

Q31b. If yes, what metrics do you use to determine the effectiveness of your TPRM assessment program? Please select all that apply.	North America	APAC	EMEA	GLOBAL
Increase in assessments completed	54%	45%	48%	49%
Percentage of complete/accurate assessments	38%	37%	35%	37%
Fewer regulatory violations/fines	31%	18%	29%	26%
Sufficient staffing	47%	29%	33%	36%
Accurate risk & criticality categorization	27%	24%	23%	25%
Effective corrective actions, remediation, escalation	28%	18%	15%	20%
Other	2%	0%	1%	1%

Q32a. Does your organization budget allocate funds to support its third-party cybersecurity risk assessment program?	North America	APAC	EMEA	GLOBAL
Yes	43%	33%	36%	37%
No	55%	64%	60%	60%
Unsure	2%	3%	4%	3%
Total	**100%**	**100%**	**100%**	**100%**

Q32b. If yes, please provide your best estimate for the total budget dedicated for your organization's Third-Party Risk Management program this year?	North America	APAC	EMEA	GLOBAL
Less than $50,000	0%	0%	0%	0%
$50,000 to $100,000	7%	9%	10%	9%
$100,001 to $500,000	21%	23%	27%	23%
$500,001 to $1,000,000	23%	27%	30%	27%
$1,000,001 to $5,000,000	26%	24%	27%	26%
$5,000,001 to $10,000,000	19%	9%	4%	11%
$10,000,001 to $50,000,000	4%	8%	2%	4%
$50,000,001 to $100,000,000	0%	0%	0%	0%
More than $100,000,000	0%	0%	0%	0%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated average	**$3,645,750**	**$4,073,250**	**$2,023,500**	**$3,083,000**

Part 7. AI in TPRM

Q33. Has your organization adopted AI tools as part of its Third-Party Risk Management program? Please select one choice only.	North America	APAC	EMEA	GLOBAL
Yes, fully	21%	19%	18%	19%
Yes, partially	29%	21%	24%	25%
Will adopt in the next 12 months	21%	25%	23%	23%
Will adopt – no timeline	14%	13%	14%	14%
No plans	15%	22%	21%	19%
Total	**100%**	**100%**	**100%**	**100%**

Q34. What are the primary benefits realized or expected from using AI for third-party risk assessment? Please select three choices only.	North America	APAC	EMEA	GLOBAL
Better prioritization	36%	33%	39%	36%
Management of third-party risk programs	41%	44%	42%	42%
Real-time intelligence to identify vulnerabilities	46%	48%	49%	48%
Improved TPRM efficiency	35%	37%	39%	37%
Frees staff for higher-value work	54%	55%	49%	53%
Reduces likelihood of third-party breach	34%	32%	35%	34%
Improves documentation	28%	29%	28%	28%
Extends ability to assess 100 percent of third parties	21%	18%	16%	18%
Other	5%	4%	3%	4%

Part 8. Demographics

D1. What organizational level best describes your current position?	North America	APAC	EMEA	GLOBAL
Executive/VP	8%	7%	9%	8%
Director	20%	18%	21%	20%
Manager	22%	26%	23%	24%
Supervisor	15%	14%	11%	13%
Staff/Technician	29%	29%	29%	29%
Contractor	6%	5%	6%	5%
Other	0%	1%	1%	1%
Total	**100%**	**100%**	**100%**	**100%**

D2. What range best describes the full-time headcount of your global organization?	North America	APAC	EMEA	GLOBAL
500 to 1,000	13%	16%	21%	17%
1,001 to 5,000	19%	27%	24%	23%
5,001 to 10,000	21%	26%	28%	25%
10,001 to 25,000	24%	17%	16%	19%
25,001 to 75,000	14%	11%	9%	11%
More than 75,000	9%	3%	2%	5%
Total	**100%**	**100%**	**100%**	**100%**

D4. What industry best describes your organization's industry focus?	North America	APAC	EMEA	GLOBAL
Agriculture & Food Services	1%	0%	2%	1%
Communications	6%	3%	4%	4%
Consumer products	7%	5%	7%	6%
Defense & Aerospace	1%	0%	2%	1%
Education	2%	2%	2%	2%
Energy & Utilities	6%	6%	9%	7%
Entertainment & Media	3%	4%	2%	3%
Financial Services	18%	14%	12%	15%
Health & Pharmaceutical	6%	6%	9%	7%
Hospitality	3%	4%	2%	3%
Industrial & Manufacturing	9%	11%	12%	11%
Public Sector	10%	11%	13%	11%
Retail	7%	4%	5%	5%
Services	7%	10%	9%	9%
Technology & Software	9%	13%	7%	10%
Transportation	3%	4%	2%	3%
Other	2%	3%	1%	2%
Total	**100%**	**100%**	**100%**	**100%**

APPENDIX 2: COMPANY SIZE

Data Tables

Company Size

What range best describes the full-time headcount of your global organization?	Overall	Less Than 10,000	More than 10,000
500 to 1,000	17%	17%	0%
1,001 to 5,000	23%	23%	0%
5,001 to 10,000	25%	25%	0%
10,001 to 25,000	19%	0%	19%
25,001 to 75,000	11%	0%	11%
More than 75,000	5%	0%	5%
Total	**100%**	**65%**	**35%**

Part 1. Background on your Portfolio

Q1: How many third parties are in your portfolio?	Overall	Less Than 10,000	More than 10,000
Less than 500	29%	29%	0%
501 to 1,000	28%	28%	0%
1,001 to 5,000	23%	23%	0%
5,000 to 10,000	15%	0%	15%
More than 10,000	5%	0%	5%
Total	**100%**	**80%**	**20%**

Q2. What percent of your total third-party population **should you** assess? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Less than 10 percent	23%	13%	33%
10 percent to 25 percent	25%	26%	24%
26 percent to 50 percent	19%	20%	18%
51 percent to 75 percent	14%	15%	13%
76 percent to 100 percent	19%	26%	12%
Total	**100%**	**100%**	**100%**

Q3. What percent of your total third-party population do you assess? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Less than 10 percent	23%	26%	21%
10 percent to 25 percent	29%	28%	30%
26 percent to 50 percent	15%	15%	16%
51 percent to 75 percent	18%	16%	19%
76 percent to 100 percent	15%	15%	14%
Total	**100%**	**100%**	**100%**

Q5. Do you have an inherent risk process that determines the frequency of third-party risk assessments?	Overall	Less Than 10,000	More than 10,000
Yes	52%	52%	53%
No	48%	48%	47%
Total	**100%**	**100%**	**100%**

Q6. If yes, do you scope your assessment questionnaire or employ a specific questionnaire based on the third-party's inherent risk?	Overall	Less Than 10,000	More than 10,000
Yes	53%	44%	61%
No	47%	56%	39%
Total	**100%**	**100%**	**100%**

Part 2. Operating Model and Methods

Q8. How would you rate the maturity of your TPRM program? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Ad hoc or informal: There are only a few defined processes in place for third-party assessments	22%	28%	15%
Reactive: Assessments are defined for key third parties, but they are still manual and inconsistent	30%	32%	29%
Proactive: Assessments are standardized and repeatable for most third parties with defined policies, tools, and remediation processes	29%	23%	35%
Optimized: The TPRM program is fully embedded in business operations using automation, advanced analytics, and continuous monitoring to manage vendor risk proactively	19%	17%	21%
Total	**100%**	**100%**	**100%**

Q9. What type of questionnaire do you use to assess your third parties? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
We developed the questionnaire	25%	23%	27%
We use an industry-standard questionnaire such as SIG, CAIQ	26%	26%	26%
Compliance/regulations	24%	25%	23%
We use a combination of our own questionnaire and an industry-standard questionnaire	24%	24%	24%
Other	1%	2%	0%
Total	**100%**	**100%**	**100%**

Q10. What tools or platforms do you currently use to conduct third-party risk assessments? Please select all that apply.	Overall	Less Than 10,000	More than 10,000
Spreadsheets	64%	63%	64%
Homegrown/IT built tools	67%	69%	66%
GRC Platform	61%	55%	66%
Dedicated TPRM Platform	58%	48%	69%
Managed Service/outsourced	45%	41%	50%
Other	5%	4%	6%

Q11. In addition to questionnaires, which data sources does your TPRM team use when assessing third parties?	Overall	Less Than 10,000	More than 10,000
Vendor documentation of practices and policies	51%	45%	58%
Independent ratings of the organization's cybersecurity and risk posture	45%	47%	42%
Threat intelligence feeds	47%	50%	45%
Financial statements and reports	28%	26%	29%
Regulatory reports or publicly available compliance data	31%	32%	30%
Service level agreements (SLA)	62%	63%	62%
Environmental, Social, and Governance (ESG)	16%	16%	15%
Other	2%	3%	2%

Part 3. Processes and Performance

Q14. On average, how long does it take to complete one third-party assessment (from launch to closure)?	Overall	Less Than 10,000	More than 10,000
Less than 30 days	21%	23%	20%
1 to 3 months	19%	22%	16%
4 to 6 months	23%	21%	25%
7 to 12 months	24%	21%	26%
More than 12 months	13%	13%	13%
Total	**100%**	**100%**	**100%**

Q15. On average, how many hours of your team's time does one third-party assessment take? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Less than 8 hours (1 day)	10%	10%	9%
8 to 40 hours (1 week)	27%	26%	29%
41 to 160 hours (1 month)	35%	38%	31%
More than 160 hours	28%	26%	31%
Total	**100%**	**100%**	**100%**

Q16. How long do vendors typically take to respond to your questionnaires? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Less than 7 days	10%	12%	7%
7 days to 1 month	12%	11%	13%
1 to 3 months	17%	17%	17%
4 to 6 months	23%	20%	27%
7 to 12 months	18%	19%	16%
More than 12 months	20%	21%	20%
Total	**100%**	**100%**	**100%**

Q17a. Do you currently have a backlog of third-party assessments?	Overall	Less Than 10,000	More than 10,000
Yes	40%	45%	36%
No	60%	55%	64%
Total	**100%**	**100%**	**100%**

Q17b. If yes, what are the primary causes of backlogs in your assessment process? Please select all that apply.	Overall	Less Than 10,000	More than 10,000
Lack of vendor response	64%	69%	60%
Incomplete information from vendor	67%	65%	69%
Limited resources such as lack of budget, technology, and in-house expertise	62%	66%	58%
Other	4%	4%	4%

Q18. What percentage of third-party responses require further attention or follow up with the third party? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Less than 10 percent	21%	21%	21%
10 percent to 25 percent	17%	15%	19%
26 percent to 50 percent	22%	22%	22%
51 percent to 75 percent	19%	19%	19%
76 percent to 100 percent	21%	23%	19%
Total	**100%**	**100%**	**100%**

Q19. How long does it typically take to remediate issues with one third party found during a third-party assessment? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Less than 7 days	11%	13%	9%
7 days to 1 month	15%	16%	14%
1 to 3 months	18%	20%	17%
4 to 6 months	20%	13%	26%
7 to 12 months	16%	12%	20%
More than 12 months	20%	26%	14%
Total	**100%**	**100%**	**100%**

Part 4. Vendor Engagement and Risk Findings

Q20. Approximately what percentage of your third parties do not respond to your assessment questionnaires?	Overall	Less Than 10,000	More than 10,000
None	7%	8%	7%
Less than 5 percent	12%	12%	12%
5 percent to 10 percent	16%	14%	18%
11 percent to 25 percent	20%	19%	20%
26 percent to 50 percent	22%	24%	20%
More than 50 percent	23%	23%	23%
Total	**100%**	**100%**	**100%**

Q21. How often do you receive updates on changes in vendor risk posture (continous monitoring)? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Nightly	9%	7%	11%
Weekly	11%	11%	11%
Monthly	17%	17%	17%
Quarterly	18%	20%	16%
Yearly	27%	26%	28%
Never	18%	19%	17%
Total	**100%**	**100%**	**100%**

Q22. Approximately what percentage of your third parties require remediation activities during the onboarding process to meet your security and privacy requirements?	Overall	Less Than 10,000	More than 10,000
None	6%	6%	7%
Less than 5 percent	13%	13%	12%
5 percent to 10 percent	19%	17%	22%
11 percent to 25 percent	18%	19%	15%
26 percent to 50 percent	22%	23%	21%
More than 50 percent	22%	22%	23%
Total	**100%**	**100%**	**100%**

Q23. On average, what percentage of remediation activities are completed prior to onboarding?	Overall	Less Than 10,000	More than 10,000
No remediation activities are completed prior to onboarding	18%	16%	21%
1 percent to 25 percent of the third parties that required remediation are completed	22%	21%	22%
26 percent to 50 percent of the third parties that required remediation activities are completed	22%	24%	18%
51 percent to 90 percent of the third parties that required remediation activities are completed	22%	26%	19%
90 percent to 100 percent of the third parties that required remediation activities are completed	16%	13%	20%
Total	**100%**	**100%**	**100%**

Q24. If only 50 percent or less of remediation activities are completed, what were the reasons that prevented the completion of remediation before onboarding? Please select all that apply.	Overall	Less Than 10,000	More than 10,000
Technical dependency on another team or provider	59%	59%	59%
Automation gaps	48%	63%	34%
Data access issues	56%	60%	53%
Immediate need to engage third party	46%	49%	42%
Expedited request (where risk is accepted)	30%	33%	28%
Resource constraints (staff's time)	67%	71%	63%
Budget limits	29%	39%	18%
Other	4%	4%	4%

Part 5. Governance and Team

Q25. Which function is most responsible for third-party risk assessments in your organization? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Procurement	14%	14%	14%
Information Technology	22%	23%	21%
Information Security / Cybersecurity	30%	27%	32%
The Third-Party Risk Management team	20%	21%	19%
Risk and Compliance	12%	12%	13%
Other	2%	3%	1%
Total	**100%**	**100%**	**100%**

Q27. How many FTEs (full-time equivalents) are dedicated to vendor risk assessments in your organization?	Overall	Less Than 10,000	More than 10,000
None	6%	8%	5%
1 to 5	40%	49%	31%
6 to 10	33%	23%	44%
11 to 20	13%	7%	18%
21 to 50	5%	8%	2%
More than 50	3%	5%	0%
Total	**100%**	**100%**	**100%**

Q27a. Do you outsource any part of the assessment process (e.g., collection, validation, monitoring)?	Overall	Less Than 10,000	More than 10,000
Yes	43%	54%	32%
No	57%	46%	68%
Total	**100%**	**100%**	**100%**

Q27b. If yes, what part of the assessment process do you outsource? Please select all that apply.	Overall	Less Than 10,000	More than 10,000
Collection	59%	57%	62%
Validation	44%	43%	45%
Monitoring	59%	55%	62%
Other	2%	1%	2%

Part 6. Outcomes, Maturity, and Budget

Q28. How effective are your organzation's third-party risk assessments in reducing the likelihood of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1=not effective to 10=highly effective.	Overall	Less Than 10,000	More than 10,000
1 or 2	10%	11%	8%
3 or 4	16%	20%	12%
5 or 6	21%	29%	14%
7 or 8	23%	16%	29%
9 or 10	30%	24%	37%
Total	**100%**	**100%**	**100%**

Q29a. How many data breaches or security incidents caused by third parties did your organization experience over the past 12 months?	Overall	Less Than 10,000	More than 10,000
None	10%	8%	11%
1 to 5	25%	29%	21%
6 to 10	17%	17%	17%
11 to 20	24%	23%	25%
21 to 30	15%	14%	16%
More than 30	5%	6%	4%
Unsure	4%	3%	6%
Total	**100%**	**100%**	**100%**

Q29b. If yes, what were the consequences of the third-party data breach or security incident? Please select all that apply.	Overall	Less Than 10,000	More than 10,000
Financial loss	52%	48%	56%
Operational disruptions	64%	63%	65%
Reputational damage	42%	42%	41%
Lawsuits and fines	16%	14%	18%
Regulatory consequences	19%	21%	18%
Intellectual property theft	30%	28%	33%
Strategic setbacks	15%	14%	17%
Other	4%	4%	4%

Q30a. Did your third parties alert you to any security incidents generated by fourth parties in the last 12 months?	Overall	Less Than 10,000	More than 10,000
Yes	41%	38%	44%
No	59%	62%	56%
Total	**100%**	**100%**	**100%**

Q30b. If yes, how many alerts did you receive in the past 12 months?	Overall	Less Than 10,000	More than 10,000
None	0%	0%	0%
1 to 5	19%	19%	20%
6 to 10	21%	21%	22%
11 to 20	31%	29%	33%
21 to 30	23%	24%	21%
More than 30	6%	7%	4%
Total	**100%**	**100%**	**100%**

Q31a. Does your organization measure the effectiveness of your TPRM assessment program?	Overall	Less Than 10,000	More than 10,000
Yes	49%	38%	61%
No	51%	62%	39%
Total	**100%**	**100%**	**100%**

Q31b. If yes, what metrics do you use to determine the effectiveness of your TPRM assessment program? Please select all that apply.	Overall	Less Than 10,000	More than 10,000
Increase in assessments completed	49%	55%	43%
Percentage of complete/accurate assessments	37%	37%	36%
Fewer regulatory violations/fines	26%	18%	34%
Sufficient staffing	36%	29%	44%
Accurate risk & criticality categorization	25%	24%	25%
Effective corrective actions, remediation, escalation	20%	18%	23%
Other	1%	0%	2%

Q32a. Does your organization budget allocate funds to support its third-party cybersecurity risk assessment program?	Overall	Less Than 10,000	More than 10,000
Yes	37%	33%	42%
No	60%	64%	55%
Unsure	3%	3%	3%
Total	**100%**	**100%**	**100%**

Q32b. If yes, please provide your best estimate for the total budget dedicated for your organization's Third-Party Risk Management program this year?	Overall	Less Than 10,000	More than 10,000
Less than $50,000	0%	0%	0%
$50,000 to $100,000	9%	4%	13%
$100,001 to $500,000	23%	23%	23%
$500,001 to $1,000,000	27%	27%	27%
$1,000,001 to $5,000,000	26%	24%	29%
$5,000,001 to $10,000,000	11%	17%	5%
$10,000,001 to $50,000,000	4%	5%	3%
$50,000,001 to $100,000,000	0%	0%	0%
More than $100,000,000	0%	0%	0%
Total	**100%**	**100%**	**100%**

Part 7. AI in TPRM

Q33. Has your organization adopted AI tools as part of its Third-Party Risk Management program? Please select one choice only.	Overall	Less Than 10,000	More than 10,000
Yes, fully	19	19	20
Yes, partially	25	21	28
Will adopt in the next 12 months	23	25	21
Will adopt – no timeline	14	13	14
No plans	19	22	17
Total	**100%**	**100%**	**100%**

Q34. What are the primary benefits realized or expected from using AI for third-party risk assessment? Please select three choices only.	Overall	Less Than 10,000	More than 10,000
Better prioritization	36%	33%	39%
Management of third-party risk programs	42%	44%	41%
Real-time intelligence to identify vulnerabilities	48%	48%	47%
Improved TPRM efficiency	37%	37%	37%
Frees staff for higher-value work	53%	55%	50%
Reduces likelihood of third-party breach	34%	32%	35%
Improves documentation	28%	29%	28%
Extends ability to assess 100 percent of third parties	18%	18%	19%
Other	4%	4%	4%

Part 8. Demographics

D1. What organizational level best describes your current position?	Overall	Less Than 10,000	More than 10,000
Executive/VP	8%	7%	9%
Director	20%	18%	22%
Manager	24%	26%	22%
Supervisor	13%	14%	13%
Staff/Technician	29%	29%	29%
Contractor	5%	5%	5%
Other	1%	1%	0%
Total	**100%**	**100%**	**100%**

D2. What range best describes the full-time headcount of your global organization?	Overall	Less Than 10,000	More than 10,000
500 to 1,000	17%	16%	17%
1,001 to 5,000	23%	27%	20%
5,001 to 10,000	25%	26%	24%
10,001 to 25,000	19%	17%	21%
25,001 to 75,000	11%	11%	12%
More than 75,000	5%	3%	6%
Total	**100%**	**100%**	**100%**

D4. What industry best describes your organization's industry focus?	Overall	Less Than 10,000	More than 10,000
Agriculture & Food Services	1%	0%	2%
Communications	4%	3%	6%
Consumer products	6%	5%	8%
Defense & aerospace	1%	0%	2%
Education	2%	2%	2%
Energy & utilities	7%	6%	8%
Entertainment & media	3%	4%	2%
Financial services	15%	14%	15%
Health & pharmaceutical	7%	6%	8%
Hospitality	3%	4%	2%
Industrial & manufacturing	11%	11%	10%
Public sector	11%	11%	12%
Retail	5%	4%	7%
Services	9%	10%	7%
Technology & software	10%	13%	6%
Transportation	3%	4%	2%
Other	2%	3%	1%
Total	**100%**	**100%**	**100%**

APPENDIX 3: INDUSTRY

Data Tables

2026 Survey Responses

D4. What industry best describes your organization's industry focus?	Percentage
Financial Services (FS)	15.0%
Public Sector (PS)	11.0%
Industrial & Manufacturing (IM)	11.0%
Technology & Software (TS)	10.0%
Services (SV)	9.0%
Health & Pharmaceutical (HP)	7.0%
Retail (RT)	5.0%

Part 1. Background on your Portfolio

Q1: How many third parties are in your portfolio?	FS	PS	IM	TS	SV	HP	RT
Less than 500	23%	22%	31%	34%	37%	28%	28%
501 to 1,000	29%	25%	23%	19%	29%	28%	32%
1,001 to 5,000	25%	30%	21%	28%	18%	20%	19%
5,000 to 10,000	20%	18%	17%	14%	13%	18%	16%
More than 10,000	3%	5%	8%	5%	3%	6%	5%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q2. What percent of your total third-party population **should you** assess? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Less than 10 percent	20%	28%	25%	22%	16%	21%	26%
10 percent to 25 percent	26%	19%	28%	25%	27%	29%	23%
26 percent to 50 percent	20%	16%	19%	19%	22%	18%	18%
51 percent to 75 percent	17%	14%	13%	14%	16%	14%	15%
76 percent to 100 percent	17%	23%	15%	20%	19%	18%	18%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q3. What percent of your total third-party population **do you** assess? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Less than 10 percent	24%	23%	24%	25%	21%	21%	25%
10 percent to 25 percent	27%	30%	30%	26%	32%	28%	33%
26 percent to 50 percent	15%	16%	16%	17%	14%	16%	12%
51 percent to 75 percent	16%	20%	18%	18%	21%	17%	16%
76 percent to 100 percent	18%	11%	12%	14%	12%	18%	14%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q5. Do you have an inherent risk process that determines the frequency of third-party risk assessments?	FS	PS	IM	TS	SV	HP	RT
Yes	53%	49%	54%	57%	54%	59%	48%
No	47%	51%	46%	43%	46%	41%	52%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q6. If yes, do you scope your assessment questionnaire or employ a specific questionnaire based on the third-party's inherent risk?	FS	PS	IM	TS	SV	HP	RT
Yes	64%	44%	59%	55%	39%	60%	44%
No	36%	56%	41%	45%	61%	40%	56%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Part 2. Operating Model and Methods

Q8. How would you rate the maturity of your TPRM program? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Ad hoc or informal: There are only a few defined processes in place for third-party assessments	31%	20%	19%	23%	26%	23%	24%
Reactive: Assessments are defined for key third parties but they are still manual and inconsistent	27%	30%	31%	29%	29%	29%	32%
Proactive: Assessments are standardized and repeatable for most third parties with defined policies, tools, and remediation processes	24%	32%	27%	28%	29%	27%	26%
Optimized: The TPRM program is fully embedded in business operations using automation, advanced analytics, and continuous monitoring to manage vendor risk proactively	18%	18%	23%	20%	16%	21%	18%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q9. What type of questionnaire do you use to assess your third parties? Please select only one choice.	FS	PS	IM	TS	SV	HP	RT
We developed the questionnaire	25%	27%	25%	23%	26%	23%	24%
We use an industry-standard questionnaire such as SIG, CAIQ	26%	25%	23%	30%	29%	29%	28%
Compliance/regulations	26%	24%	26%	22%	22%	24%	21%
We use a combination of our own questionnaire and an industry-standard questionnaire	23%	23%	26%	23%	23%	23%	26%
Other	0%	1%	0%	2%	0%	1%	1%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q10. What tools or platforms do you currently use to conduct third-party risk assessments? Please select all that apply.	FS	PS	IM	TS	SV	HP	RT
Spreadsheets	60%	63%	60%	61%	69%	62%	64%
Homegrown/IT built tools	65%	70%	64%	65%	66%	65%	61%
GRC Platform	62%	59%	59%	62%	64%	59%	64%
Dedicated TPRM Platform	56%	63%	56%	58%	57%	55%	58%
Managed Service/ outsourced	48%	49%	47%	47%	46%	41%	42%
Other	7%	5%	7%	6%	5%	4%	6%

Q11. In addition to questionnaires, which data sources does your TPRM team use when assessing third parties?	FS	PS	IM	TS	SV	HP	RT
Vendor documentation of practices and policies	41%	55%	43%	47%	53%	51%	49%
Independent ratings of the organization's cybersecurity and risk posture	45%	38%	41%	40%	54%	43%	45%
Threat intelligence feeds	53%	44%	49%	50%	47%	43%	51%
Financial statements and reports	29%	31%	27%	28%	26%	29%	27%
Regulatory reports or publicly available compliance data	30%	25%	27%	27%	29%	28%	29%
Service Level Agreements (SLA)	65%	54%	59%	57%	67%	65%	58%
Environmental, Social, and Governance (ESG)	18%	14%	15%	18%	17%	16%	21%
Other	4%	1%	3%	2%	3%	2%	2%

Q12. Do you assess fourth-party (subcontractor) risk as part of your TPRM program?	FS	PS	IM	TS	SV	HP	RT
Yes	26%	25%	25%	24%	29%	26%	23%
Only for critical suppliers	18%	17%	20%	18%	16%	18%	22%
No	56%	58%	55%	58%	55%	56%	55%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q13. Do you feel confident that you have visibility into the fourth parties that could impact your company? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Not confident, no trust	36%	13%	19%	23%	21%	21%	20%
Slight confidence, minimal assurance with significant doubts	16%	20%	12%	16%	14%	15%	17%
Moderately confident, somewhat assured	12%	11%	13%	9%	14%	14%	10%
Confident, only minor reservations	16%	20%	29%	22%	17%	21%	22%
Highly confident, complete trust in visibility	20%	36%	27%	30%	34%	29%	31%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Part 3. Processes and Performance

Q14. On average, how long does it take to complete one third-party assessment (from launch to closure)?	FS	PS	IM	TS	SV	HP	RT
Less than 30 days	24%	20%	22%	20%	10%	12%	25%
1 to 3 months	18%	19%	16%	12%	21%	23%	18%
4 to 6 months	25%	25%	25%	25%	23%	23%	23%
7 to 12 months	21%	23%	22%	30%	30%	29%	22%
More than 12 months	12%	13%	15%	13%	16%	13%	12%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q15. On average, how many hours of your team's time does one third-party assessment take? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Less than 8 hours (1 day)	10%	8%	8%	9%	11%	9%	12%
8 to 40 hours (1 week)	26%	27%	35%	26%	28%	29%	28%
41 to 160 hours (1 month)	38%	34%	30%	36%	34%	35%	36%
More than 160 hours	26%	31%	27%	29%	27%	27%	24%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q16. How long do vendors typically take to respond to your questionnaires? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Less than 7 days	12%	8%	10%	10%	12%	9%	10%
7 days to 1 month	11%	12%	12%	11%	15%	14%	9%
1 to 3 months	17%	15%	16%	16%	17%	13%	16%
4 to 6 months	20%	26%	22%	23%	20%	19%	24%
7 to 12 months	19%	16%	18%	18%	17%	21%	19%
More than 12 months	21%	23%	22%	22%	19%	24%	22%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q17a. Do you currently have a backlog of third-party assessments?	FS	PS	IM	TS	SV	HP	RT
Yes	45%	32%	40%	39%	38%	41%	35%
No	55%	68%	60%	61%	62%	59%	65%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q17b. If yes, what are the primary causes of backlogs in your assessment process? Please select all that apply.	FS	PS	IM	TS	SV	HP	RT
Lack of vendor response	71%	63%	57%	65%	58%	56%	62%
Incomplete information from vendor	65%	68%	67%	67%	64%	67%	61%
Limited resources such as lack of budget, technology, and in-house expertise	66%	59%	62%	62%	67%	65%	58%
Other	4%	6%	5%	5%	6%	5%	7%

Q18. What percentage of third-party responses require further attention or follow up with the third party? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Less than 10 percent	22%	21%	23%	24%	19%	23%	24%
10 percent to 25 percent	13%	18%	17%	18%	20%	14%	15%
26 percent to 50 percent	25%	20%	19%	23%	23%	25%	19%
51 percent to 75 percent	17%	15%	18%	17%	19%	20%	17%
76 percent to 100 percent	23%	26%	23%	18%	19%	18%	25%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q19. How long does it typically take to remediate issues with one third party found during a third-party assessment? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Less than 7 days	13%	9%	12%	20%	23%	13%	14%
7 days to 1 month	10%	11%	13%	11%	10%	12%	15%
1 to 3 months	22%	17%	20%	13%	23%	17%	10%
4 to 6 months	21%	23%	22%	22%	10%	21%	26%
7 to 12 months	17%	18%	18%	15%	23%	25%	24%
More than 12 months	17%	22%	15%	19%	11%	12%	11%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Part 4. Vendor Engagement and Risk Findings

Q20. Approximately what percentage of your third parties do not respond to your assessment questionnaires?	FS	PS	IM	TS	SV	HP	RT
None	12%	11%	13%	14%	11%	10%	10%
Less than 5 percent	14%	16%	15%	15%	12%	13%	12%
5 percent to 10 percent	14%	18%	16%	15%	18%	19%	16%
11 percent to 25 percent	19%	20%	23%	21%	18%	19%	22%
26 percent to 50 percent	18%	17%	15%	19%	22%	16%	19%
More than 50 percent	23%	18%	18%	16%	19%	23%	21%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q21. How often do you receive updates on changes in vendor risk posture (continous monitoring)? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Nightly	10%	12%	11%	13%	9%	5%	8%
Weekly	13%	10%	13%	14%	12%	13%	10%
Monthly	16%	15%	18%	16%	17%	18%	17%
Quarterly	21%	19%	15%	19%	16%	22%	17%
Yearly	24%	23%	24%	23%	29%	25%	28%
Never	16%	21%	19%	15%	17%	17%	20%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q22. Approximately what percentage of your third parties require remediation activities during the onboarding process to meet your security and privacy requirements?	FS	PS	IM	TS	SV	HP	RT
None	5%	9%	5%	7%	6%	6%	4%
Less than 5 percent	12%	12%	13%	12%	14%	12%	13%
5 percent to 10 percent	18%	19%	21%	23%	21%	19%	24%
11 percent to 25 percent	20%	19%	21%	18%	18%	17%	16%
26 percent to 50 percent	23%	23%	20%	21%	21%	21%	22%
More than 50 percent	22%	18%	20%	19%	20%	25%	21%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q23. On average, what percentage of remediation activities are completed prior to onboarding?	FS	PS	IM	TS	SV	HP	RT
No remediation activities are completed prior to onboarding	16%	20%	18%	18%	19%	21%	15%
1 percent to 25 percent of the third parties that required remediation activities are completed	21%	23%	22%	22%	25%	27%	23%
26 percent to 50 percent of the third parties that required remediation activities are completed	24%	18%	21%	21%	19%	15%	22%
51 percent to 90 percent of the third parties that required remediation activities are completed	26%	20%	23%	23%	23%	17%	26%
90 percent to 100 percent of the third parties that required remediation activities are completed	13%	19%	16%	16%	14%	20%	14%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q24. If only 50 percent or less of remediation activities are completed, what were the reasons that prevented the completion of remediation before onboarding? Please select all that apply.	FS	PS	IM	TS	SV	HP	RT
Technical dependency on another team or provider	54%	50%	56%	65%	58%	61%	56%
Automation gaps	44%	49%	47%	45%	46%	49%	52%
Data access issues	58%	56%	56%	54%	54%	55%	50%
Immediate need to engage third party	41%	49%	43%	41%	42%	44%	46%
Expedited request (where risk is accepted)	29%	32%	39%	33%	28%	33%	26%
Resource constraints (staff's time)	71%	62%	63%	65%	68%	69%	59%
Budget limits	36%	23%	33%	21%	25%	23%	25%
Other	3%	5%	4%	5%	4%	3%	6%

Part 5. Governance and Team

Q25. Which function is most responsible for third-party risk assessments in your organization? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Procurement	15%	14%	13%	16%	16%	15%	14%
Information Technology	23%	20%	21%	17%	19%	20%	20%
Information Security / Cybersecurity	28%	32%	33%	29%	30%	31%	30%
The Third-Party Risk Management team	23%	21%	17%	19%	18%	21%	23%
Risk and Compliance	8%	13%	16%	16%	16%	13%	10%
Other	3%	0%	0%	3%	1%	0%	3%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q26. How many FTEs (full-time equivalents) are dedicated to vendor risk assessments in your organization?	FS	PS	IM	TS	SV	HP	RT
None	4%	5%	9%	4%	5%	7%	6%
1 to 5	38%	41%	34%	29%	39%	47%	49%
6 to 10	34%	36%	38%	37%	28%	26%	25%
11 to 20	15%	12%	11%	16%	14%	13%	12%
21 to 50	7%	5%	4%	8%	8%	4%	6%
More than 50	2%	1%	4%	6%	6%	3%	2%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q27a. Do you outsource any part of the assessment process (e.g., collection, validation, monitoring)?	FS	PS	IM	TS	SV	HP	RT
Yes	42%	45%	48%	45%	40%	43%	46%
No	58%	55%	52%	55%	60%	57%	54%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q27b. If yes, what part of the assessment process do you outsource? Please select all that apply.	FS	PS	IM	TS	SV	HP	RT
Collection	60%	62%	56%	56%	63%	60%	53%
Validation	43%	42%	43%	43%	41%	42%	44%
Monitoring	56%	58%	58%	61%	60%	58%	59%
Other	1%	3%	2%	3%	4%	3%	5%

Part 6. Outcomes, Maturity, and Budget

Q28. How effective are your organization's third-party risk assessments in reducing the likelihood of a third-party data breach? Please use the following 10-point scale to express your opinion, from 1= not effective to 10 = highly effective.	FS	PS	IM	TS	SV	HP	RT
1 or 2	11%	9%	10%	10%	15%	11%	9%
3 or 4	10%	24%	17%	17%	16%	15%	18%
5 or 6	19%	22%	21%	21%	18%	20%	24%
7 or 8	26%	21%	22%	25%	22%	24%	23%
9 or 10	34%	24%	30%	27%	29%	30%	26%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q29a. How many data breaches or security incidencts caused by third parties did your organization experience over the past 12 months?	FS	PS	IM	TS	SV	HP	RT
None	10%	8%	13%	9%	13%	10%	8%
1 to 5	26%	23%	23%	27%	25%	26%	24%
6 to 10	19%	15%	18%	15%	19%	19%	20%
11 to 20	23%	27%	23%	23%	24%	23%	23%
21 to 30	14%	18%	14%	14%	12%	12%	15%
More than 30	6%	4%	5%	8%	4%	4%	5%
Unsure	2%	5%	4%	4%	3%	6%	5%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q29b. If yes, what were the consequences of the third-party data breach or security incident? Please select all that apply.	FS	PS	IM	TS	SV	HP	RT
Financial loss	51%	54%	53%	51%	57%	49%	52%
Operational disruptions	62%	63%	64%	61%	60%	67%	65%
Reputational damage	41%	44%	41%	42%	43%	44%	43%
Lawsuits and fines	19%	20%	15%	14%	21%	16%	17%
Regulatory consequences	21%	15%	20%	24%	16%	18%	19%
Intellectual property theft	29%	34%	31%	28%	30%	32%	29%
Strategic setbacks	14%	15%	16%	13%	14%	17%	18%
Other	5%	3%	6%	4%	6%	2%	2%

Q30a. Did your third parties alert you to any security incidents generated by fourth parties in the last 12 months?	FS	PS	IM	TS	SV	HP	RT
Yes	38%	42%	38%	40%	44%	40%	37%
No	62%	58%	62%	60%	56%	60%	63%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q30b. If yes, how many alerts did you receive in the past 12 months?	FS	PS	IM	TS	SV	HP	RT
None	0%	0%	0%	0%	0%	0%	0%
1 to 5	20%	20%	22%	19%	18%	17%	22%
6 to 10	21%	22%	23%	25%	20%	19%	17%
11 to 20	29%	31%	31%	27%	32%	33%	32%
21 to 30	23%	25%	19%	24%	26%	27%	25%
More than 30	7%	2%	5%	5%	4%	4%	4%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q31a. Does your organization measure the effectiveness of your TPRM assessment program?	FS	PS	IM	TS	SV	HP	RT
Yes	40%	58%	49%	48%	51%	46%	44%
No	60%	42%	51%	52%	49%	54%	56%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q31b. If yes, what metrics do you use to determine the effectiveness of your TPRM assessment program? Please select all that apply.	FS	PS	IM	TS	SV	HP	RT
Increase in assessments completed	46%	50%	45%	50%	49%	49%	45%
Percentage of complete/ accurate assessments	37%	39%	31%	36%	42%	41%	35%
Fewer regulatory violations/ fines	28%	32%	31%	19%	21%	19%	22%
Sufficient staffing	35%	34%	38%	31%	36%	37%	35%
Accurate risk & criticality categorization	29%	27%	24%	20%	25%	23%	21%
Effective corrective actions, remediation, escalation	19%	20%	21%	18%	21%	19%	20%
Other	0%	2%	1%	1%	0%	2%	2%

Q32a. Does your organization budget allocate funds to support its third-party cybersecurity risk assessment program?	FS	PS	IM	TS	SV	HP	RT
Yes	39%	36%	33%	34%	37%	40%	35%
No	59%	59%	61%	61%	60%	57%	62%
Unsure	2%	5%	6%	5%	3%	3%	3%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q32b. If yes, please provide your best estimate for the total budget dedicated for your organization's Third-Party Risk Management program this year?	FS	PS	IM	TS	SV	HP	RT
Less than $50,000	0%	0%	0%	0%	0%	0%	0%
$50,000 to $100,000	8%	10%	9%	12%	8%	6%	7%
$100,001 to $500,000	28%	29%	29%	18%	14%	25%	20%
$500,001 to $1,000,000	28%	21%	28%	23%	23%	26%	27%
$1,000,001 to $5,000,000	23%	23%	20%	29%	31%	27%	25%
$5,000,001 to $10,000,000	11%	12%	10%	11%	10%	7%	13%
$10,000,001 to $50,000,000	2%	4%	3%	6%	12%	9%	8%
$50,000,001 to $100,000,000	0%	1%	0%	0%	2%	0%	0%
More than $100,000,000	0%	0%	1%	1%	0%	0%	0%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Part 7. AI in TPRM

Q33. Has your organization adopted AI tools as part of its Third-Party Risk Management program? Please select one choice only.	FS	PS	IM	TS	SV	HP	RT
Yes, fully	20%	18%	21%	20%	21%	18%	26%
Yes, partially	25%	27%	21%	26%	23%	20%	19%
Will adopt in the next 12 months	19%	22%	23%	20%	25%	20%	21%
Will adopt – no timeline	16%	15%	17%	15%	10%	15%	16%
No plans	20%	18%	18%	19%	21%	27%	18%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Q34. What are the primary benefits realized or expected from using AI for third-party risk assessment? Please select three choices only.	FS	PS	IM	TS	SV	HP	RT
Better prioritization	38%	35%	34%	35%	41%	37%	39%
Management of third-party risk programs	41%	42%	40%	45%	43%	43%	44%
Real-time intelligence to identify vulnerabilities	51%	49%	45%	51%	39%	47%	39%
Improved TPRM efficiency	37%	39%	39%	38%	33%	36%	37%
Frees staff for higher-value work	48%	52%	56%	50%	56%	55%	51%
Reduces likelihood of third-party breach	32%	37%	35%	35%	33%	31%	39%
Improves documentation	30%	27%	32%	25%	32%	28%	26%
Extends ability to assess 100 percent of third parties	17%	19%	16%	17%	18%	19%	20%
Other	6%	0%	3%	4%	6%	4%	5%