Prevalent™

The 2024 Prevalent Third-Party Risk Management Study

Some TPRM programs are still missing the forest for the trees.

Table of Contents

Prevalent™

Introduction

In February and March 2024, Prevalent conducted a study of current trends, challenges, and initiatives impacting third-party risk management (TPRM) practitioners worldwide.

The goal of the study was to provide a state of the market on third-party risk and deliver actionable recommendations for organizations seeking to grow and mature their TPRM programs – specifically related to improving manual processes, tools, and coverage of the third-party lifecycle and adopting new technologies such as AI to simplify TPRM.

Respondents to the study were directly involved in third-party risk management, IT vendor risk management or supplier risk management, worked for enterprises across a variety of industries and sizes in multiple geographies, and managed between 25 and 25,000 third parties.

So, how are organizations dealing with these challenges? The Prevalent 2024 Third-Party Risk Management Study has the answers.

Summary

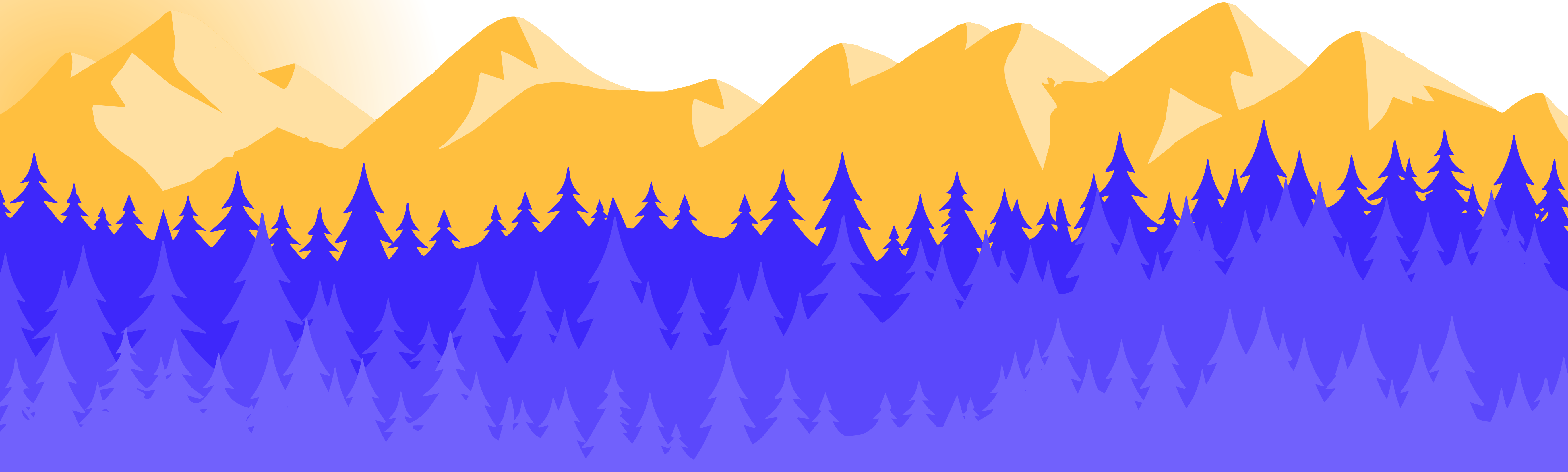
The size and scope of third-party data breaches and cybersecurity incidents increased to record levels in 2023. In fact, last year saw some of the most sizable and impactful third-party breaches and software supply chain intrusions ever, including Progress Software's MOVEit breach and continued breaches of Okta, as well as third-party cyber incidents impacting the London Metropolitan Police and LastPass that collectively affected millions of people around the world. On top of that, 1 in 3 Americans – a new record – were impacted by third-party healthcare data breaches in 2023 including those at Change Healthcare, HCA, Anthem, and Perry Johnson & Associates (PJ&A).

However, detecting and mitigating the impact of third-party cybersecurity incidents isn't the only concern for third-party risk management practitioners. Security, risk management, and compliance teams must also contend with increasing regulatory oversight and reporting regarding the use of AI, cybersecurity disclosure reporting requirements by the U.S. Securities and Exchange Commission (SEC), and expanding environmental, social and governance (ESG) and supply chain due diligence regulations – especially in Europe.

> **Given the multitude of cybersecurity incidents and emerging regulatory requirements, it's no wonder that organizations often "miss the forest for the trees" when it comes to third-party risk.**

In other words, it's easy to get caught up in the details and spend significant time, energy, and resources on a specific risk, incident, or regulation.

The results of this year's study indicate that many companies are missing a holistic approach to third-party risk management that could prevent such incidents and streamline compliance across the board. More must be done by organizations to unify their teams, solidify processes, and eliminate manual, overlapping tools to assess a greater portion of their third parties and actually remediate findings.



By analyzing these challenges in light of current best practices, we arrived at five key observations about the state of third-party risk management today:

1 Despite an overwhelming focus on managing third-party cybersecurity risks, **61% of companies reported a third-party data breach or security incident in the last 12 months – a 49% increase over last year.**

2 Although most organizations report having a TPRM program in place, **50% still rely on spreadsheets and use multiple tools to assess and manage their third parties.** Dissatisfaction with current methods could be running higher than reported.

3 Lack of resources and limited TPRM program coordination across the enterprise are obstacles to program success. As a result, organizations only **manage a third of their vendors.** There is a lot of risk hiding among the unassessed masses.

4 Later stages of the third-party lifecycle lack adequate risk assessment coverage, **and overall remediation is woefully lacking across the lifecycle – especially during pre-contract due diligence and risk assessment stages!**

5 **Only 5% of companies say they actively leverage AI in their TPRM programs.** Lack of an organizational AI strategy limits companies' use of AI in resolving long-standing TPRM challenges.

In the following pages, we share the detailed response data with further analysis and three actionable next steps from our experts.

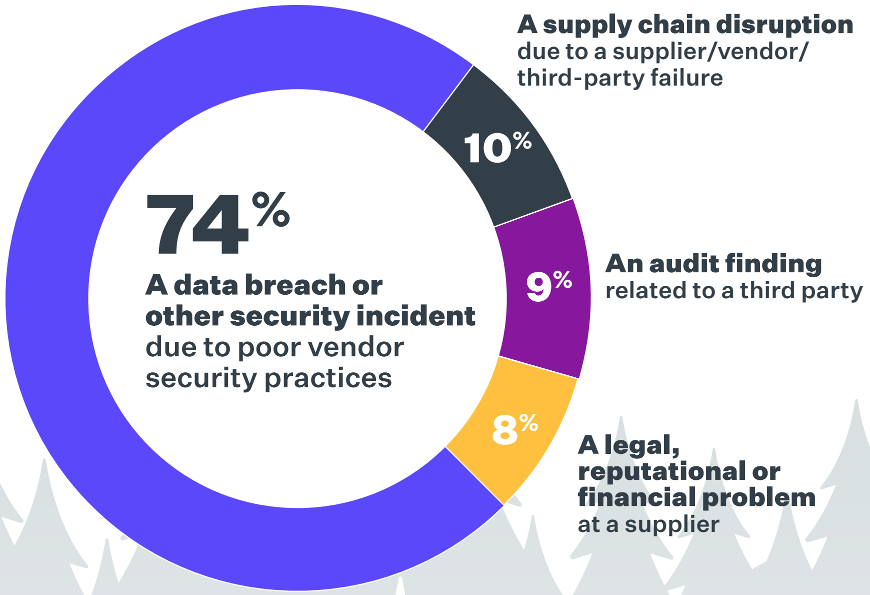
61% of companies reported a third-party data breach or security incident in the last 12 months – a 49% increase over last year.

Finding #1: Despite an overwhelming focus on managing cybersecurity risks, 61% of companies reported a third-party data breach or security incident in the last 12 months.

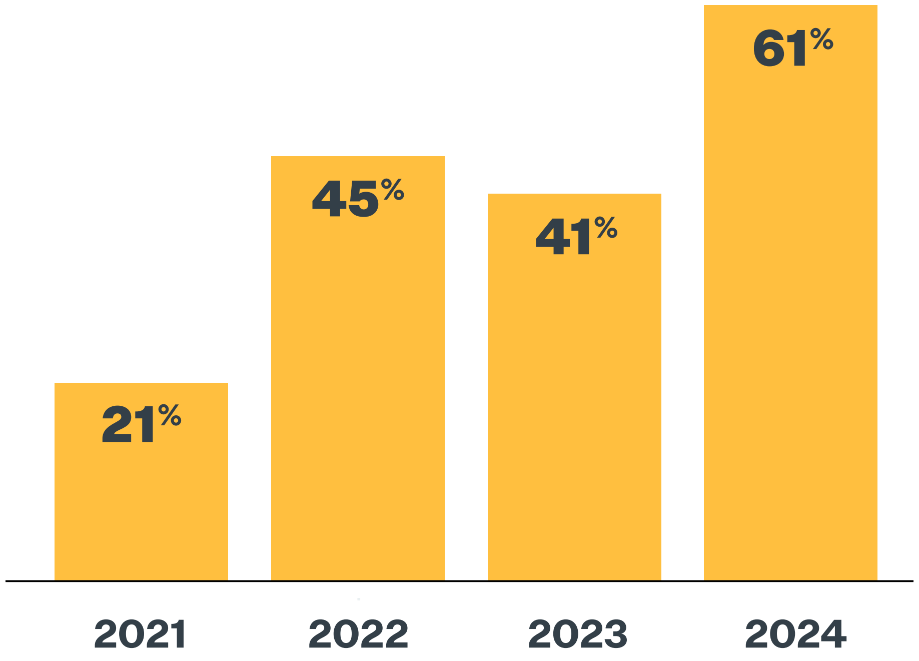
That's a 49% increase from last year. What's getting missed?

Echoing previous years' study results, the top concern facing organizations in their use of third parties – by far at 74% – is a data breach or other security incident. The reason behind this concern is quite apparent: **61% of respondents said they experienced a third-party data breach** or other security incident in the last 12 months. This represents a *significant* 49% increase over the 2023 survey results, and a three-fold increase since 2021.

What are the top concerns facing your organization regarding its usage of third parties?



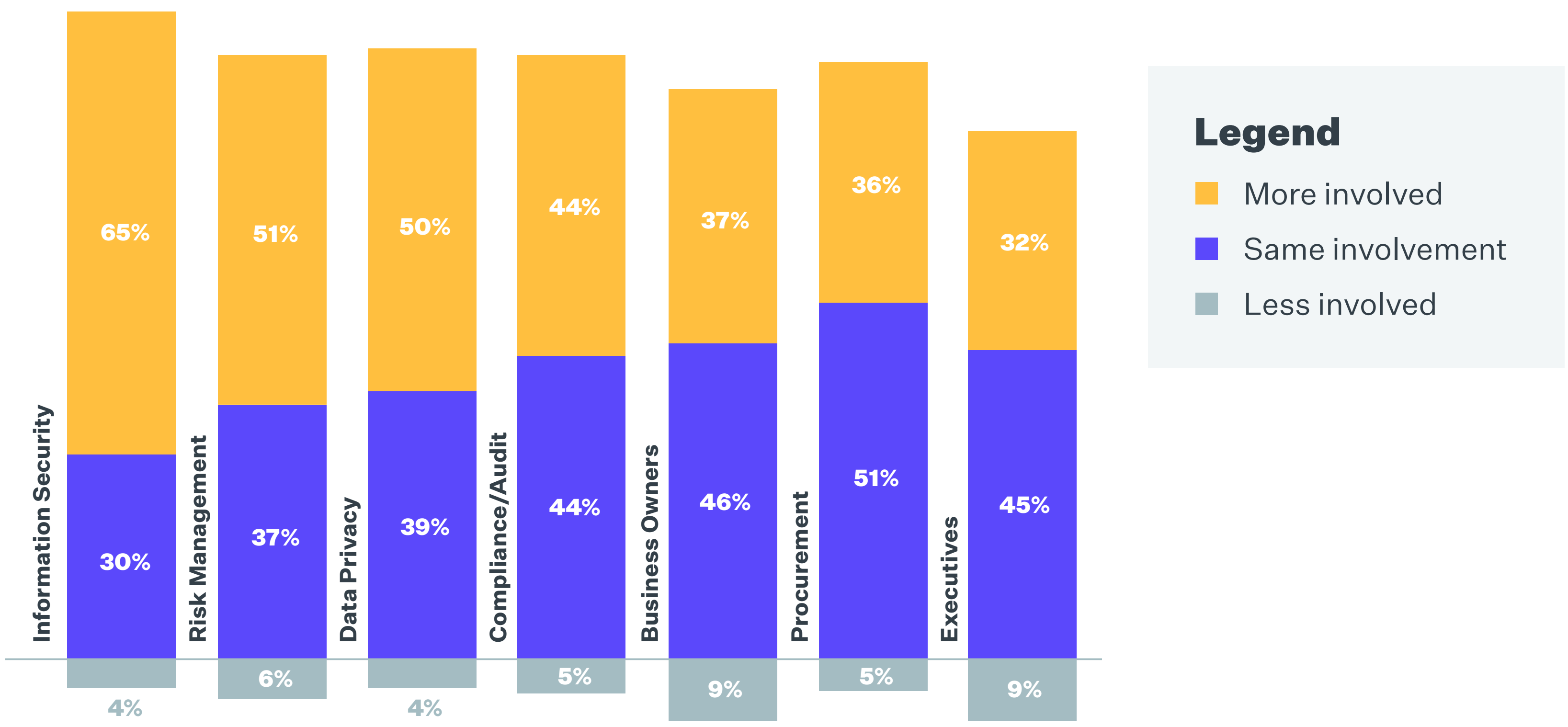
Percentage of respondents reporting a security incident related to the usage of a third party in the last 12 months.



49% YOY Increase

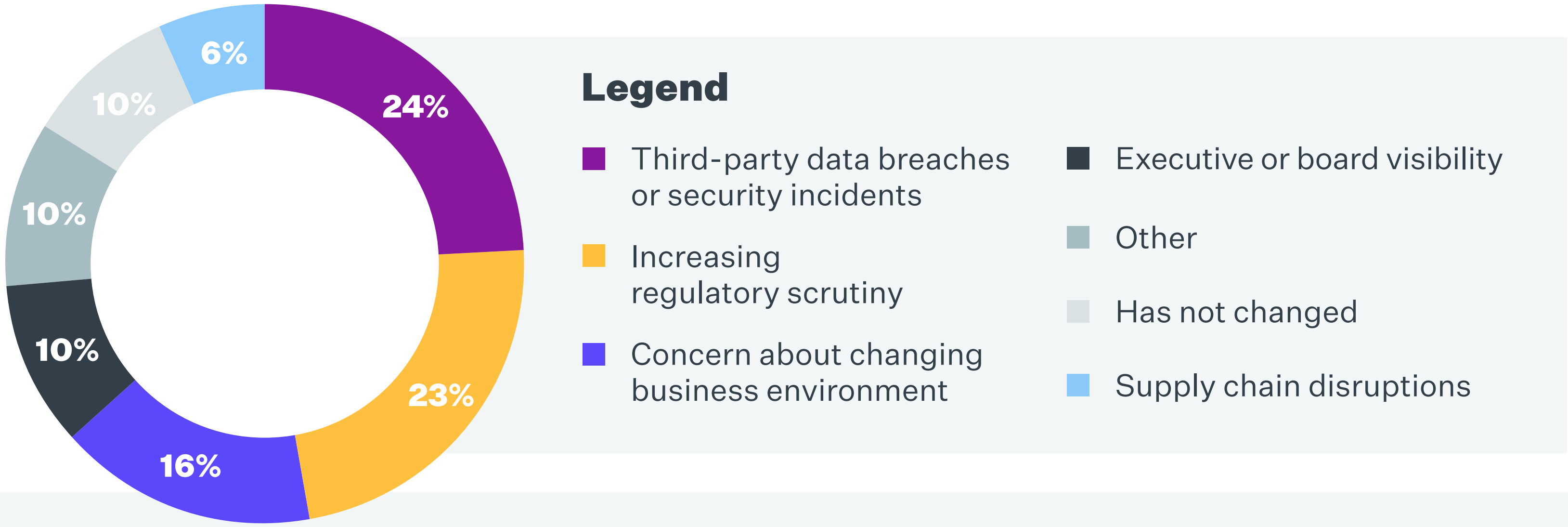
Respondents report that Information Security (65%), Risk Management (51%), and Data Privacy (50%) teams are more involved in third-party risk this year. Increased involvement across only these three teams departs from the 2023 survey, where all teams showed more participation in TPRM.

In the last year, would you say that these departments are more or less involved in third-party risk management versus the previous year?



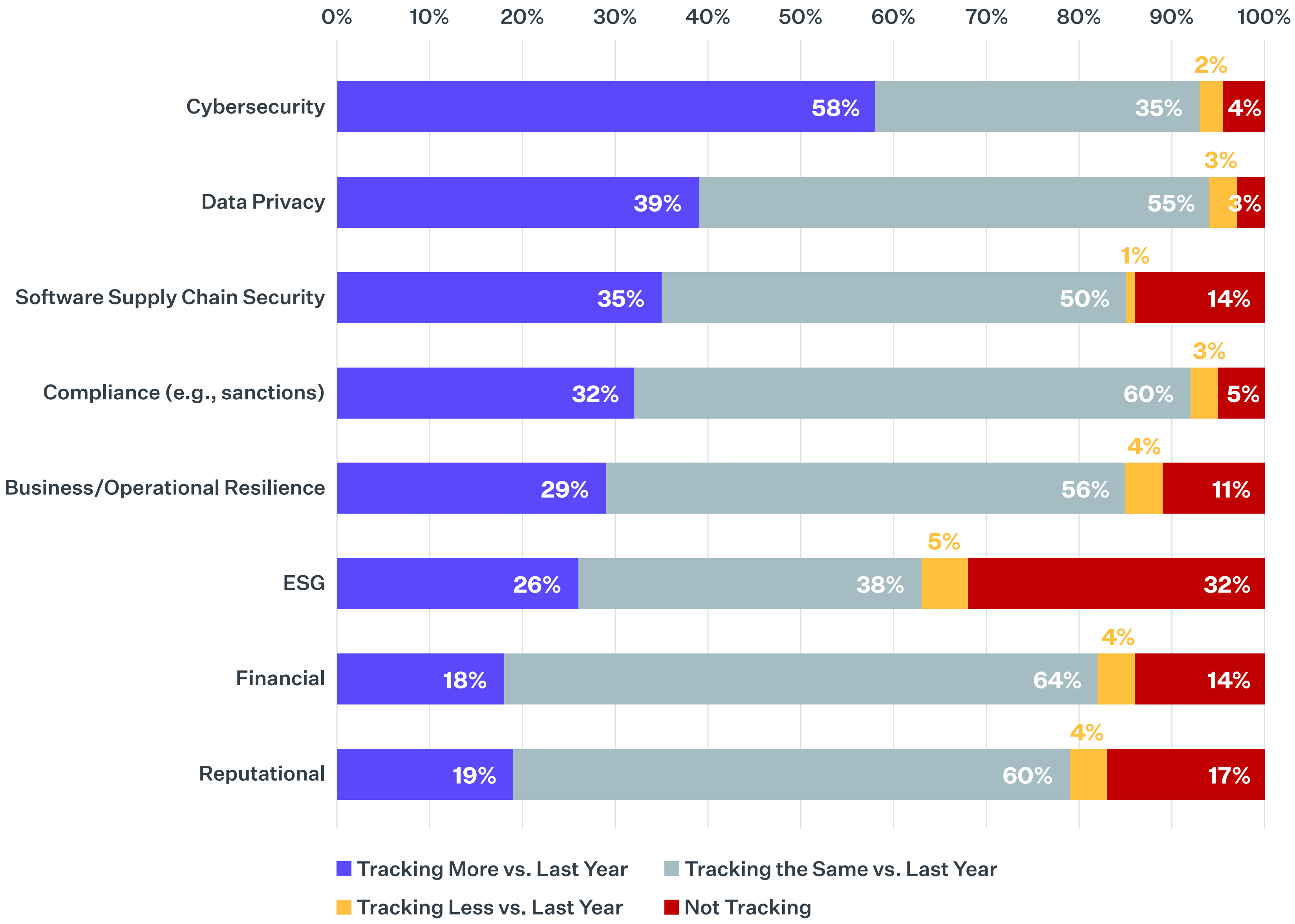
The primary reason for the increased involvement among security, risk and privacy teams was third-party data breaches or security incidents (24%) and increasing regulatory scrutiny (23%).

In general, what is the primary reason why involvement in third-party risk management has changed in the last year?



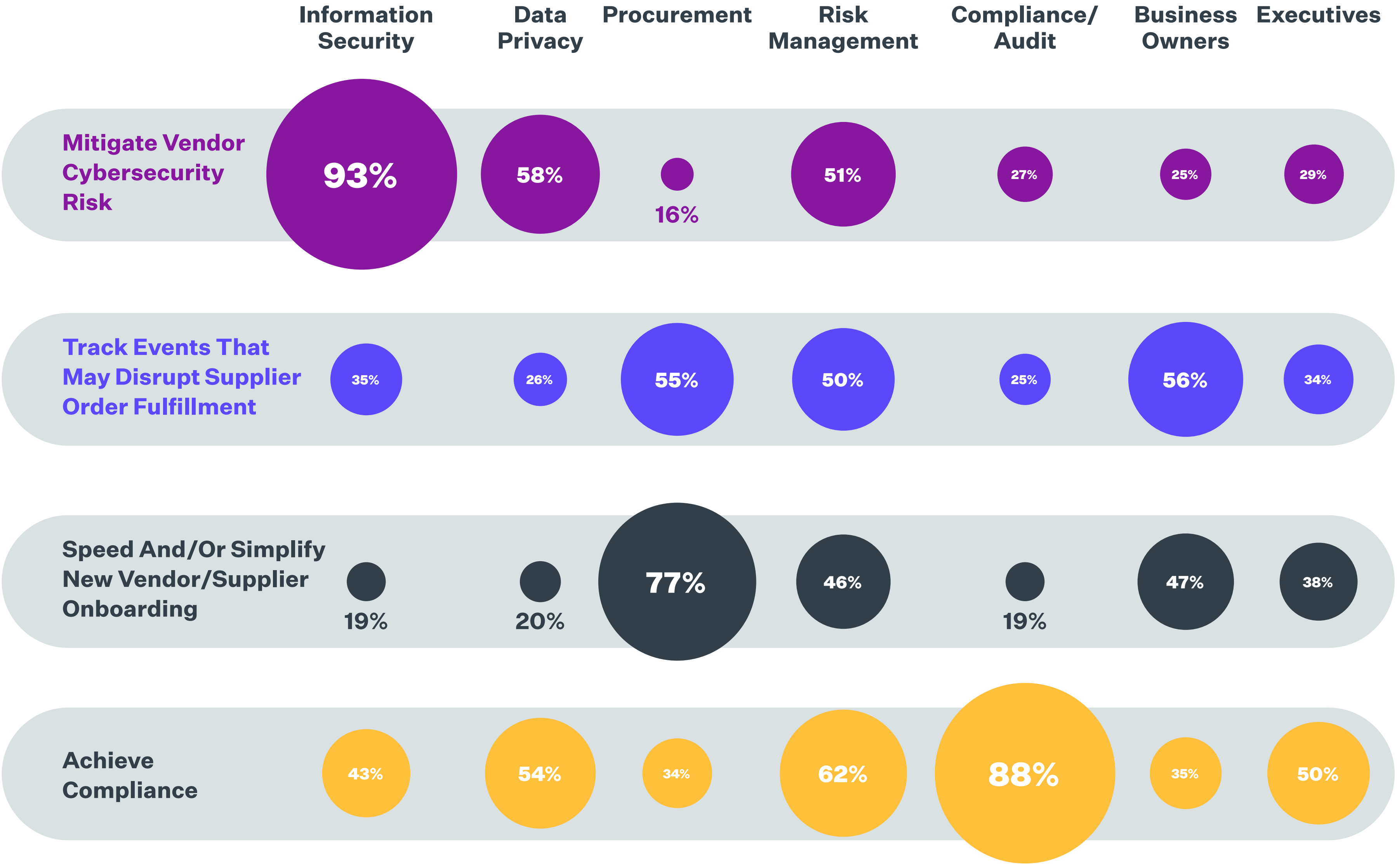
How has your organization's tracking of third-party risks changed in the last year?

In fact, the only risk type tracked this year more than last year is Cybersecurity risk (58%). Non-cyber risks like ESG are the least tracked.



Information Security teams are primarily concerned with mitigating vendor cybersecurity risks (93%). Procurement team objectives mainly focus on speeding and simplifying new vendor onboarding (77%), while 55% say that tracking events that might disrupt supplier order fulfillment is a primary objective. Both Compliance (88%) and Risk Management (62%) teams emphasize achieving compliance.

What are the primary objectives for these departments in your third-party risk management program efforts?



	Information Security	Data Privacy	Procurement	Risk Management	Compliance/ Audit	Business Owners	Executives
Mitigate Vendor Cybersecurity Risk	93%	58%	16%	51%	27%	25%	29%
Track Events That May Disrupt Supplier Order Fulfillment	35%	26%	55%	50%	25%	56%	34%
Speed And/Or Simplify New Vendor/Supplier Onboarding	19%	20%	77%	46%	19%	47%	38%
Achieve Compliance	43%	54%	34%	62%	88%	35%	50%

The Information Security team typically *owns the TPRM program.* This is consistent with the 2023 survey results, but surprisingly, Business Owners *own the third-party relationship* in this year's survey vs. in 2023 when the Procurement team owned the third-party relationship. However, data from this year's survey shows that Procurement *manages the database of vendors/suppliers.*

In your organization, which department primarily:

Owns the TPRM Program	Owns the Third-Party Relationship	Manages the Third-Party Database
1 Information Security	1 Business Owners	1 Procurement
2 Risk Management	2 Procurement	2 Information Security
3 Compliance/Audit	3 Information Security	3 Risk Management
4 Procurement	4 Compliance/Audit	4 Compliance/Audit
5 Data Privacy	5 Risk Management	5 Business Owners
6 Executives	6 Executives	6 Data Privacy
7 Business Owners	7 Data Privacy	7 Executives

The complex ownership paradigm of Security, Business Owners, and Procurement, when combined with differing departmental TPRM objectives leads to two questions:

- **Are all teams' needs being met by their current TPRM solution approach?**
- **Is remediation of risks even happening in this arrangement (and if so, who owns it)? (More on that later.)**

Finding #2:

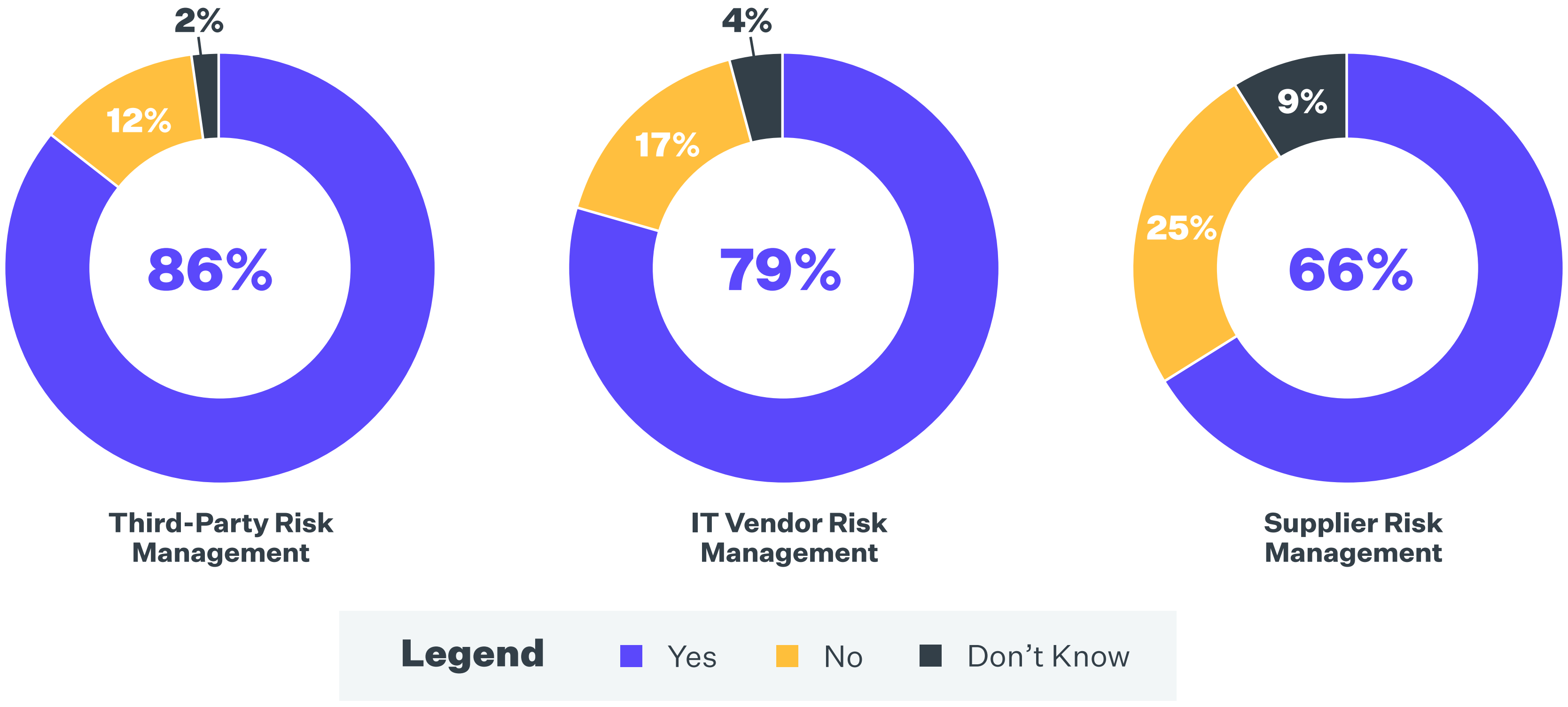
Although most organizations report having a TPRM program in place, 50% still rely on spreadsheets and use multiple tools to assess and manage their third parties.

A deeper look into current methods of assessing third parties shows that a third of the buyers are looking for a new solution – dissatisfaction with current methods could be running higher than reported.

86% of respondents indicated they have a third-party risk management (TPRM) program in place, and 79% and 66% said they had an IT vendor risk management (VRM) or supplier risk management (SRM) program in place, respectively. Organizations likely have different programs in place to address different types of third parties or risks required by different enterprise teams or departments.

However, likely owing to the predominance of Information Security ownership over TPRM programs (as noted in Finding #1), the percentage of respondents indicating they have a SRM program in place is low, and "No" and "I don't know" answers are higher.

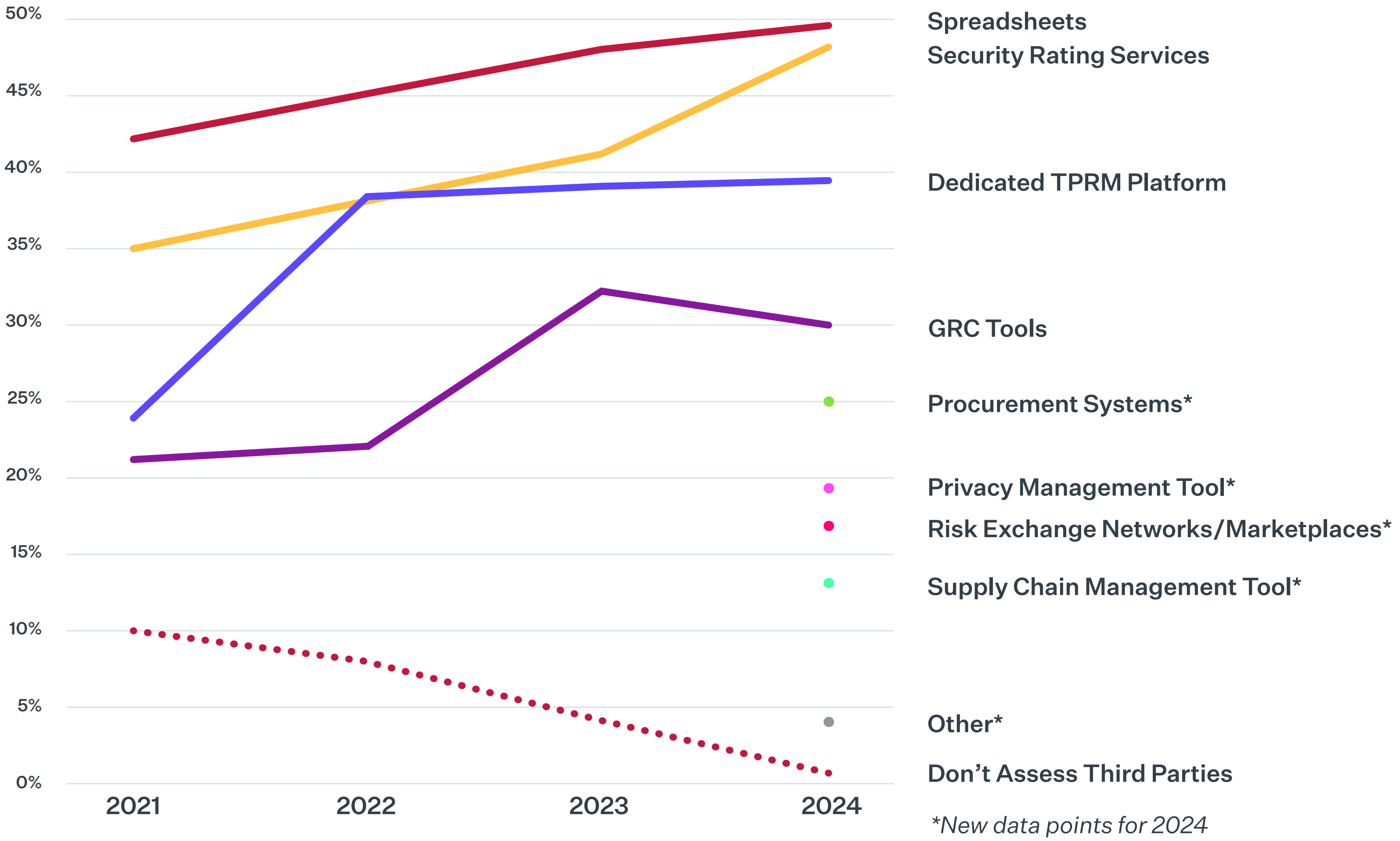
Does your organization have a third-party risk management, IT vendor risk management, or supplier risk management program in place?



Despite the vast majority of companies having a TPRM, VRM and/or SRM program in place, a frustrating half of respondents indicated that they still use spreadsheets to assess their third-party vendors and suppliers – consistent with previous years' study results. This could imply that these organizations are too involved in their established processes (i.e., the trees) to innovate or look for more integrated and efficient solutions (i.e., the forest).

The largest year-over-year growth in tool usage, however, comes from security ratings services. Growing usage of security ratings services could be tied to a greater percentage of companies that reported a third-party data breach or security incident in the last 12 months, which could lead to a need for increased visibility into cybersecurity incidents and to monitor for those risks (see Finding #1).

How do you currently assess your third parties?



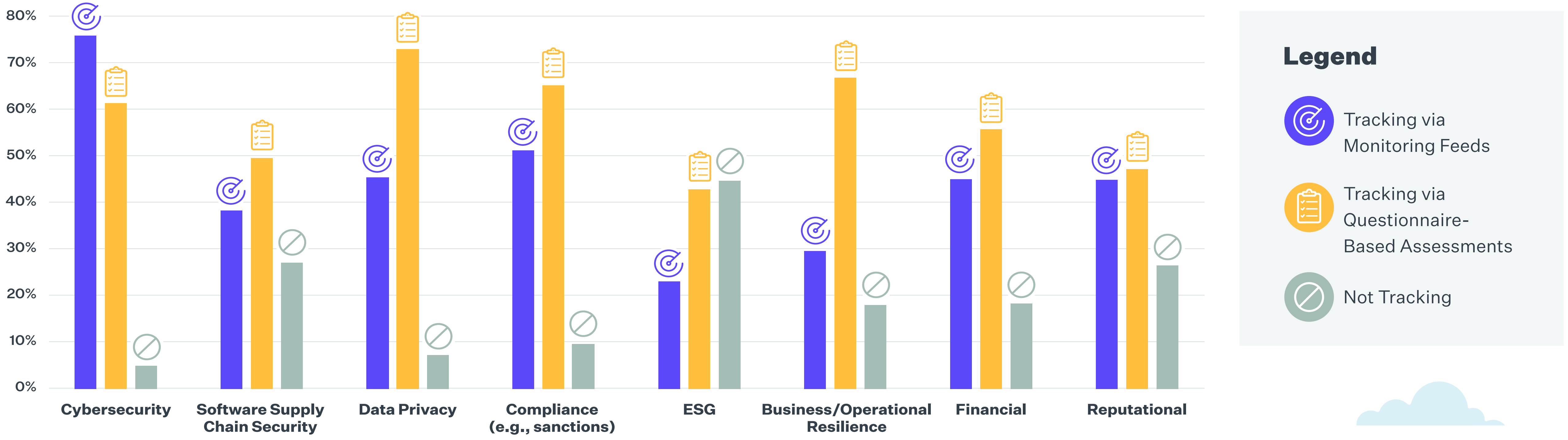
*New data points for 2024

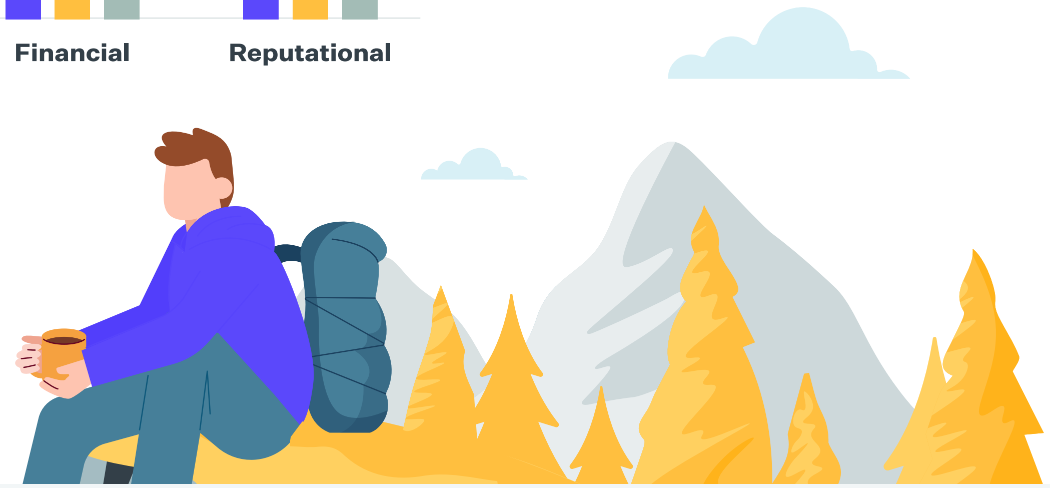
> **The key takeaway here is that organizations do not rely on a single tool to address their third-party risks – they instead use multiple tools.**

But are they the right tools? Cybersecurity is the only type of risk noted in this survey that has a higher percentage of respondents tracking via monitoring feeds (75%) vs. questionnaire-based assessments (61%).

Both methods are important, but an over-reliance on monitoring feed data could limit an organization's ability to inspect their third parties' internal controls and practices and take action to remediate those risks. The percentage of companies not tracking ESG risks (44%), software supply chain security risks (27%), and reputational risks (27%) is alarmingly high considering the potential level of damage from these types of disruptions.

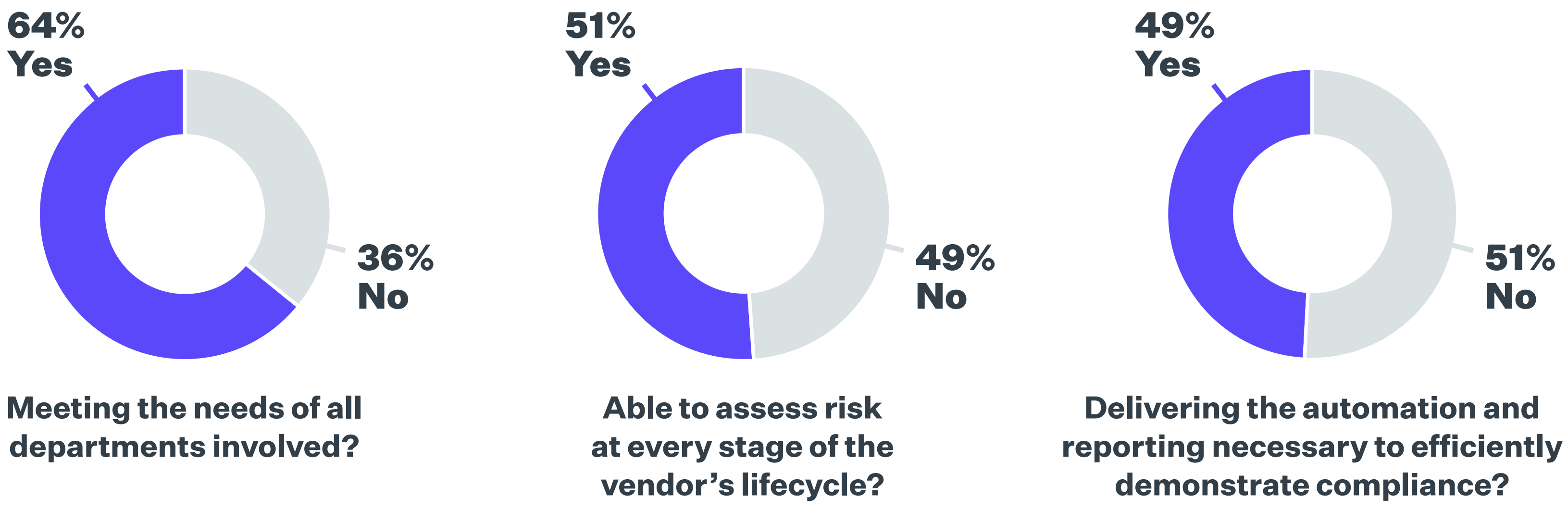
What types of third-party risks does your organization track?



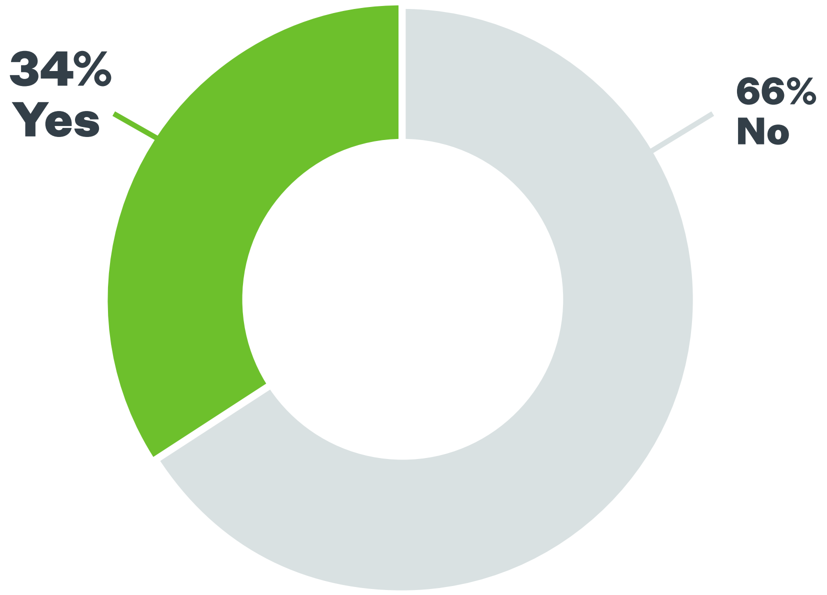


64% of organizations report that their current method of assessing third party risks meets the needs of all departments involved. However, Yes and No answer percentages start to equalize when asked if current methods are able to assess risk at every vendor lifecycle stage, and whether it delivers automation and reporting for compliance. This might explain why a third of respondents are in the market for a new solution – compliance reporting and vendor lifecycle management are important, but current tools aren't cutting it.

Is your current method of assessing third-party risk:



Are you planning to purchase, augment or replace a third-party risk management solution within the next 12 months?

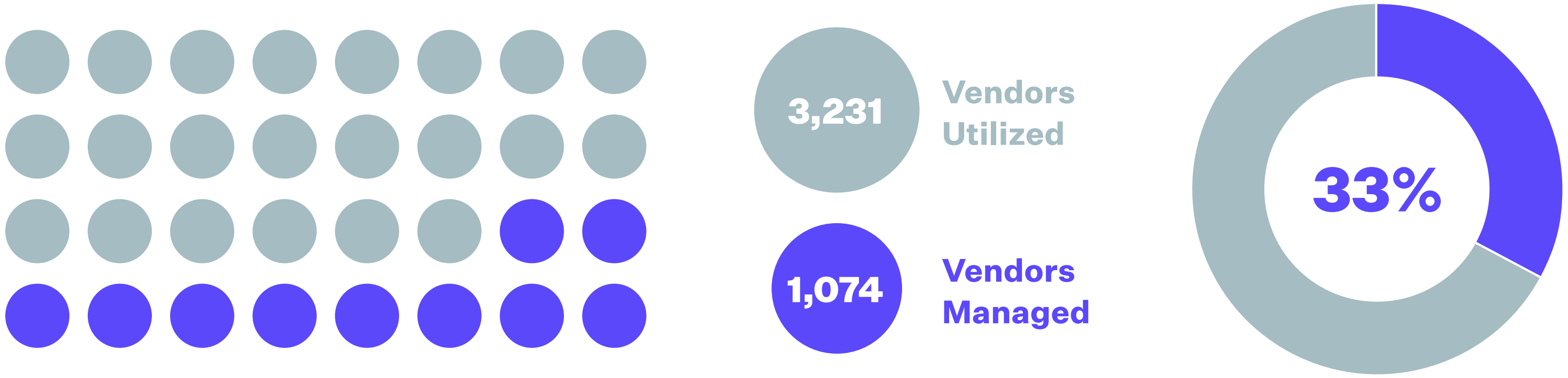


Finding #3:
Lack of resources and limited TPRM program coordination across the enterprise are obstacles to program success. As a result, organizations manage only a third of their vendors.

There is a lot of risk hiding among the unassessed masses.

Organizations only manage about 33% of the third parties they work with, or 1,074 vendors out of an average of 3,231. This might suggest that they're unable to see the larger picture of risk management due to being bogged down by the daily operational details of managing a limited number of third parties.

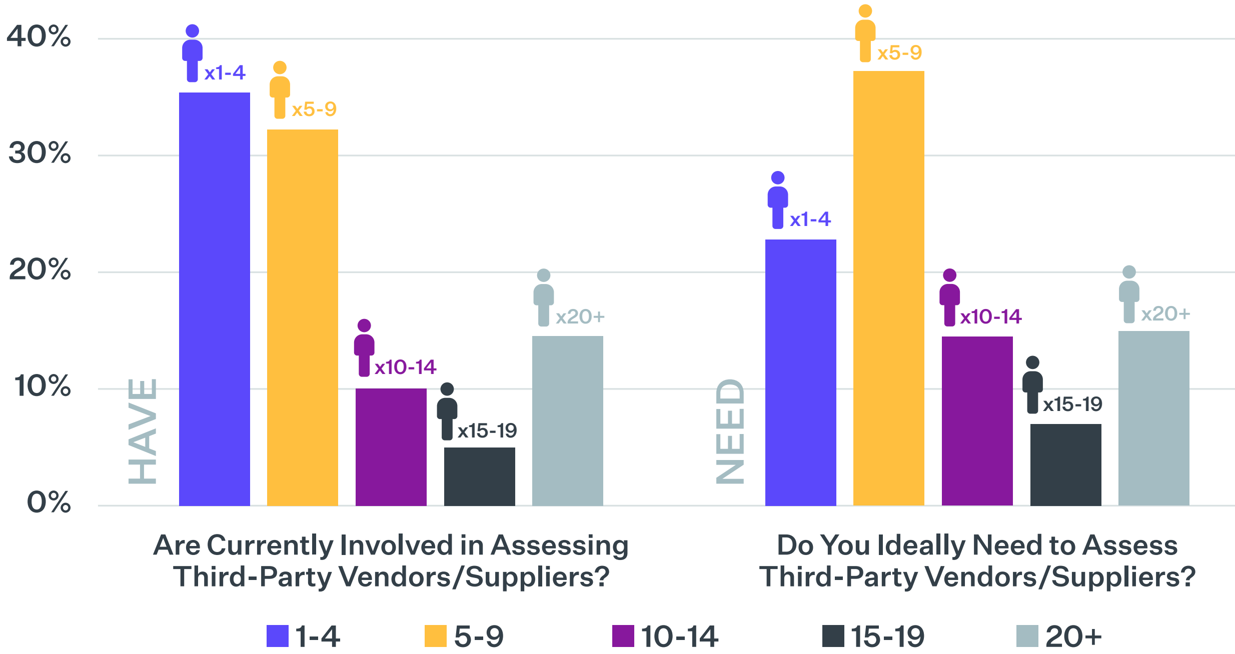
Average number of third-party vendors/suppliers utilized versus managed by organizations:



Each circle = 100 vendors

Aside from general tool and method dissatisfaction examined in Finding #2, this lack of coverage might have to do with teams responsible for assessing third parties being understaffed. 37% of respondents said they had between 1-4 people currently involved in assessing third parties, and 37% said they needed between 5-9 people. In fact, the number one barrier to TPRM program adoption or growth, as reported by 63% of respondents, is a lack of resources. Being understaffed by a factor of 2 means there are far too many unassessed vendors exposing the organization to too much risk.

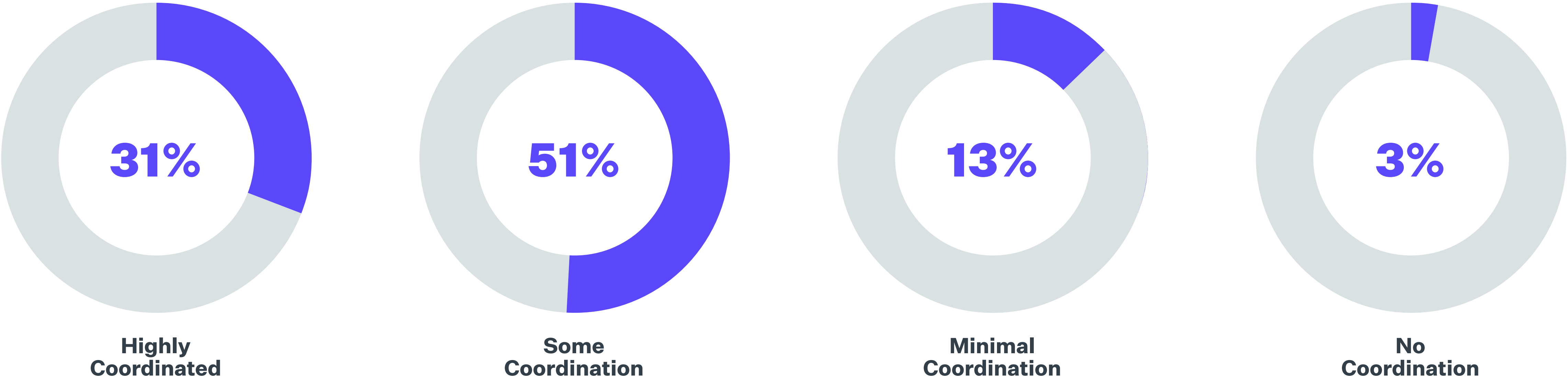
How many people in your organization:



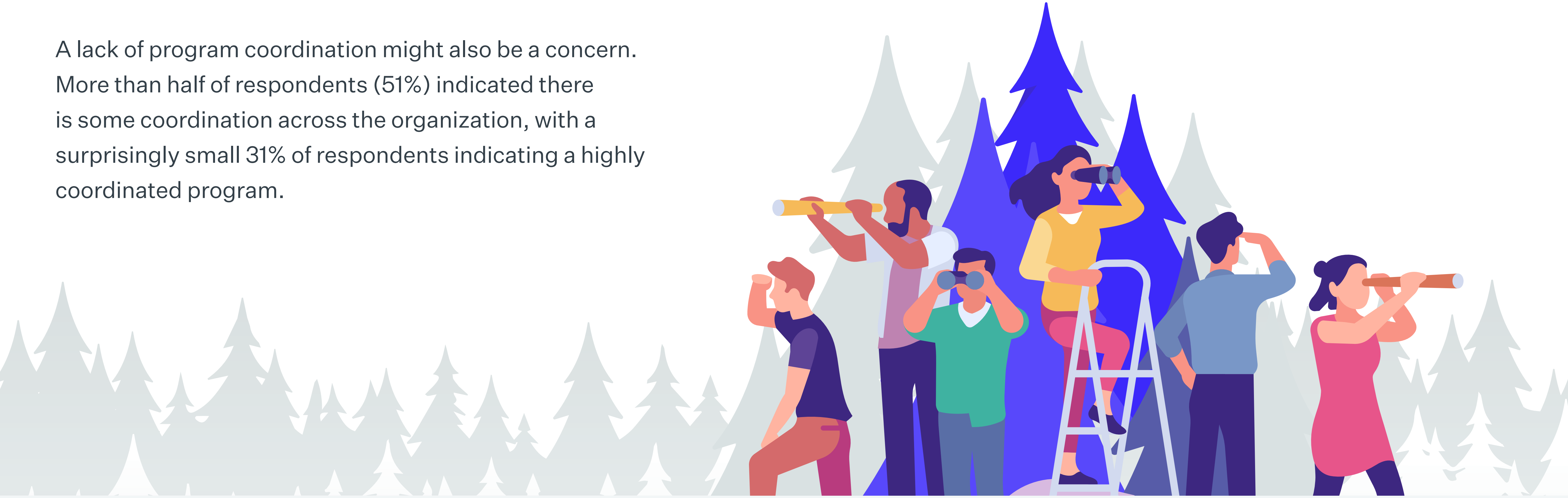
What are the barriers to adopting or growing your third-party risk management program?

#1	Lack of Resources
#2	Limited Coordination Between Departments
#3	Lack of Centralized Third-Party/ Vendor/Supplier Visibility
#4	Limited Financial Support
#5	Lack of Risk Expertise
#6	Limited Executive Support
#7	Lack of Vendor Contact Information

What is the level of program coordination across the organization for the third-party risk management/IT vendor risk management/supplier risk management program?

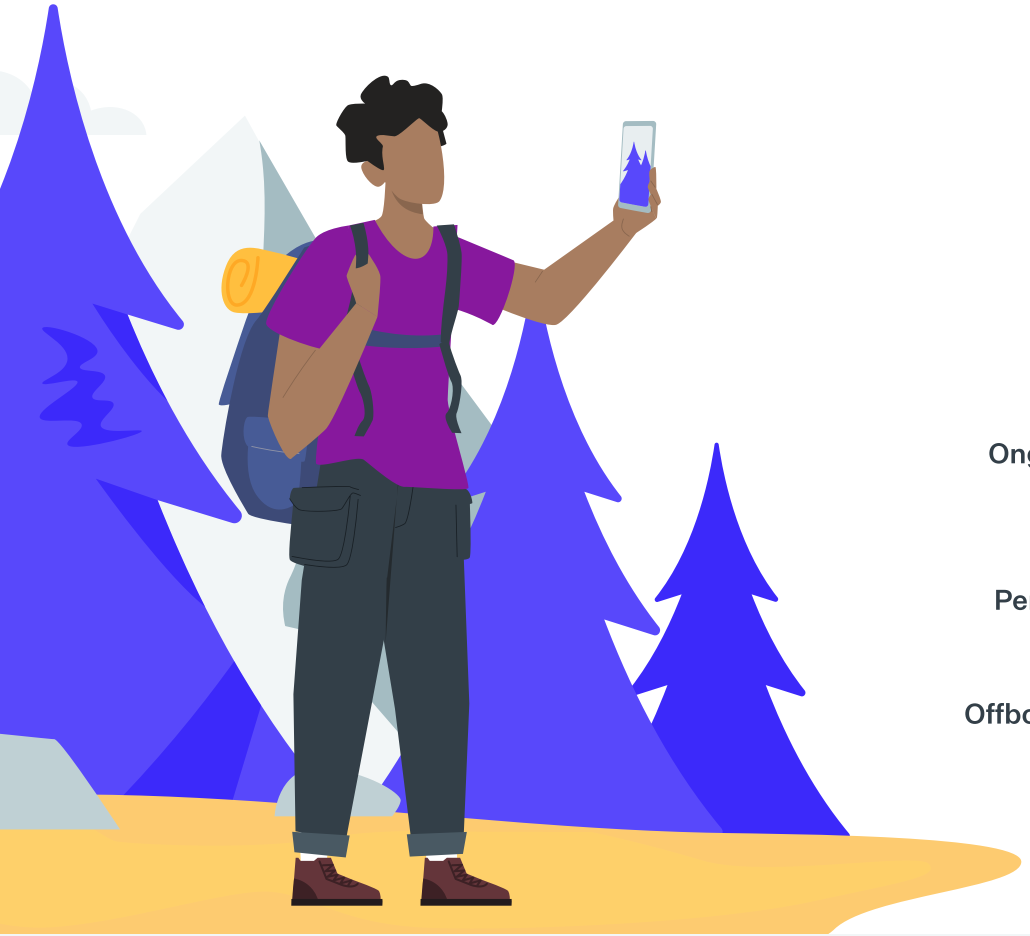


A lack of program coordination might also be a concern. More than half of respondents (51%) indicated there is some coordination across the organization, with a surprisingly small 31% of respondents indicating a highly coordinated program.



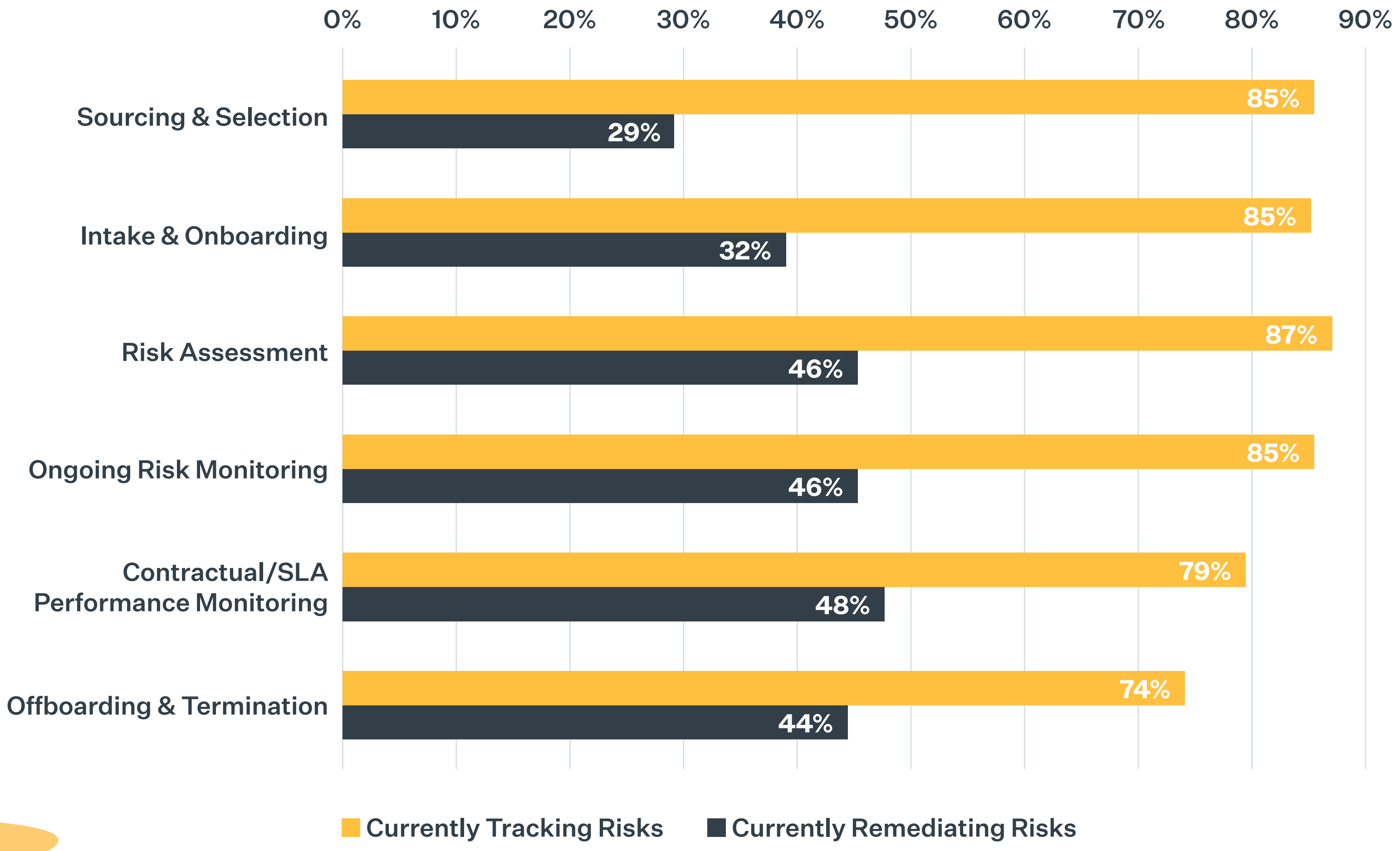
Finding #4:

Later stages of the third-party lifecycle lack adequate risk assessment coverage, and overall remediation is woefully lacking across the lifecycle.



Data from this year's study shows that between 85-87% of companies track risks from sourcing and selection through ongoing risk monitoring – an improvement over the 2023 study results – but only 74-79% of companies track SLAs and offboarding risks later in the relationship lifecycle. Although this is also an improvement over last year's study results, a lack of SLA visibility and post-contract breach risks could be problematic for organizations if they do not assess risks at these stages with the same frequency as other stages.

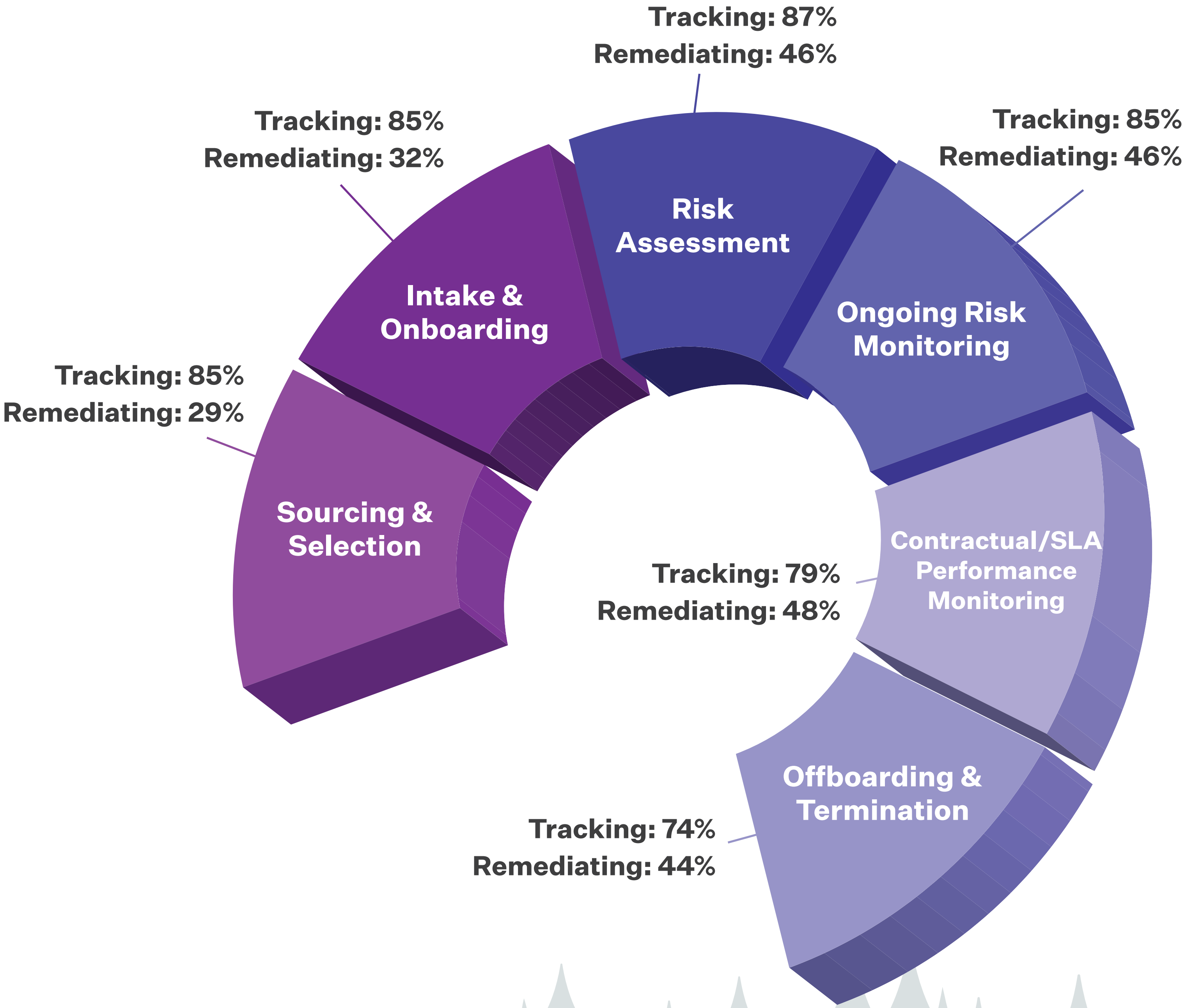
Does your organization track and/or remediate risks at the following stages in the third-party relationship lifecycle?



If companies are tracking risks adequately at the initial stages but not following through with remediation or assessment at later stages, they might be focusing too closely on the beginning of the process (trees) and missing the overall importance of full lifecycle management (forest).

What's more interesting is the disparity between the percentage of organizations tracking risks and those actually *remediating* them. Nowhere is that disparity greater than in the Sourcing and Selection stage of the life cycle. Although organizations do well in tracking risks at this stage (85%), only 29% remediate what they find.

Moreover, only 46% of companies report remediating risk as a result of Risk Assessments – the stage where risks should absolutely be mitigated!

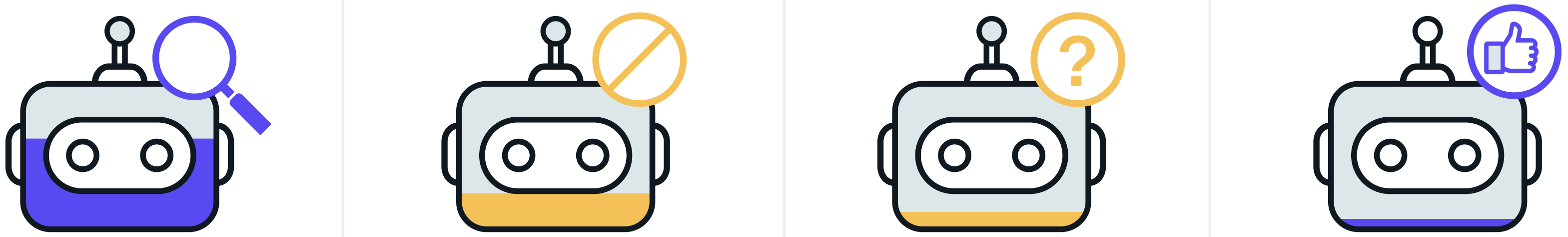


Finding #5:

Only 5% of companies say they actively use AI in their TPRM programs. Lack of an organizational AI strategy limits companies' use of AI in resolving long-standing TPRM challenges.

Although just 5% of companies say they actively use AI in their TPRM programs, 61% are investigating its use cases. 25% firmly say they have no plans to use AI. The reason why 25% of companies say they have no plans to use AI is that nearly half of them (49%) have no organizational strategy in place for AI.

Is your organization currently leveraging AI in its third-party risk management program?



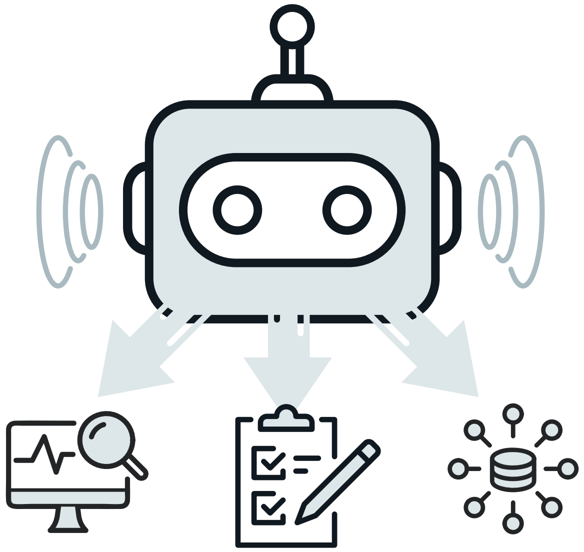
61%
No, but we are investigating its use cases.

25%
No, and and we have no plans to.

9%
Don't know

5%
Yes, we are actively using AI in our TPRM program.

Yet companies see value in AI. For organizations that are using AI or considering using it, the top use cases are around reporting, speeding up questionnaire completion, and collating data from multiple sources.



There is tremendous potential for organizations to leverage AI in their programs and may help organizations reduce the resourcing challenges exposed in Finding #3.

What are your goals with using or investigating AI for use in your TPRM program?

58%	**Extracting more valuable insights** from data for reporting
54%	**Speeding up questionnaire completion** by automatically populating surveys using existing questionnaires and available evidence
54%	**Collating and centralizing data from multiple sources** for more comprehensive vendor due diligence
38%	**Getting instant risk remediation guidance**

Why do you have no plans to use AI in your TPRM program?

49%	**No organizational strategy for AI**
19%	**Data security risks**
13%	**Lack of transparency in algorithm models**
9%	**Risks of bias or hallucination**

Recommendations

The results of this study demonstrate that third-party risk management is achieving enterprise-level visibility and importance in the face of growing third-party cybersecurity challenges, but many programs struggle with manual processes that limit risk, lifecycle, and vendor coverage. Here are three actionable steps to improve TPRM.

Create cross-functional teams and establish clear TPRM ownership to ensure that remediations are enforced

Many more organizations reported a third-party data breach or security incident this year despite an increasing organizational focus on third-party cybersecurity risks, more involvement from Information Security, Risk Management and Data Privacy teams, and greater usage of cyber monitoring tools. Why?

The underlying reason could come down to an increasingly complex ownership arrangement in most enterprises with Security owning the TPRM program, Business Owners owning the vendor relationships, and Procurement owning the operational aspects of managing vendors (e.g., onboarding).

Although most companies report having a TPRM program in place, it is unclear how well these teams collaborate within their programs. This segmented approach may be a case of teams focusing on their individual responsibilities without a collective vision, hence missing the "forest" of enterprise-wide risk management for the "trees" of department-specific goals.

While data from the study shows that there is some coordination, risk remediation is clearly lacking throughout the third-party lifecycle.

Increasing the incidence of risk remediation is critical to truly gaining the most business value from a TPRM program.

This is a good place to start to address that challenge: Create cross-functional teams with clear ownership responsibilities and extend that ownership all the way through to risk remediation. Cross-functional teams have the authority, governance, and oversight to:

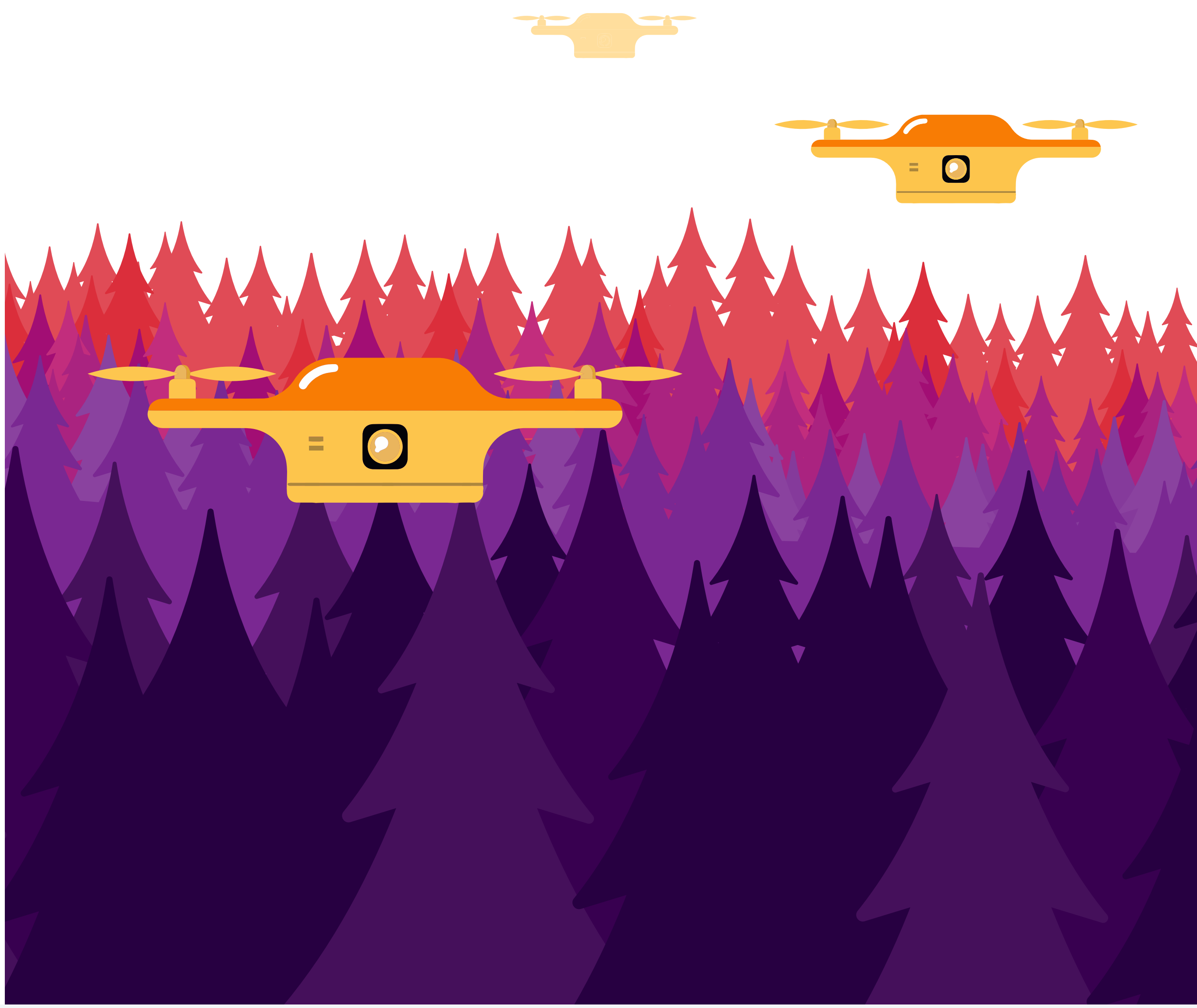
- Define and implement integrated, enterprise-wide TPRM, VRM, and SRM processes and workflows
- Establish clear roles and responsibilities (e.g., RACI) for internal and external stakeholders
- Build rules for tiering and categorizing third parties according to their criticality to the business
- Select the right risk assessment questionnaires and frameworks against which to evaluate a multitude of risks
- Refine risk scoring criteria based on the organization's risk tolerance
- Engage with auditors and executives to measure TPRM program success and adjust according to business needs
- Enforce incident response measures if a third-party data breach is discovered

Automate TPRM processes around a single platform to unify teams, data, and the risk lifecycle

Half of companies report still using spreadsheets along with a complicated set of tools to assess and manage their third parties. Although most indicate that their current solutions are meeting needs, a third of companies are in the market for new solutions. Organizations seeking new tools should seek out solutions that:

- Centralize both assessment and monitoring in a single platform
- Incorporate multiple data types (e.g., cyber, business, operational, financial, reputational, ESG, etc.) to address risks across many departmental users
- Integrate with business processes such as contract and RFx management to weave in risk with vendor management
- Offer a large library of risk assessment questionnaire templates to enable flexibility in assessing third party vendors according to the risks that matter to the organization
- Utilize built-in remediation guidance to reduce risk to an acceptable level
- Leverage automatic mapping of risks into common industry and regulatory frameworks to assist in the compliance and internal auditing processes
- Include specific capabilities to address risks across the lifecycle – from sourcing and selection of new vendors to offboarding and termination

A more comprehensive workflow-driven approach will aid in covering shortfalls in risk coverage (such as ESG and reputational risks), the risk lifecycle, and in enforcing remediations (noted in the recommendation above).



Close the resource and skill gap with outsourced managed services or artificial intelligence capabilities

Data from this year's study shows that a lack of resources is the single biggest obstacle to TPRM program success. That lack of resources translates to two-thirds of vendors not being adequately managed. To overcome resource limitations, consider outsourcing all or part of your TPRM program to expert managed services providers. Look for solutions that:

- Automate the collection of evidence and communication with vendors
- Review answers and evidence to confirm suitability and accuracy of content
- Provide remediation guidance for top identified risks
- Manage the third-party lifecycle on your behalf

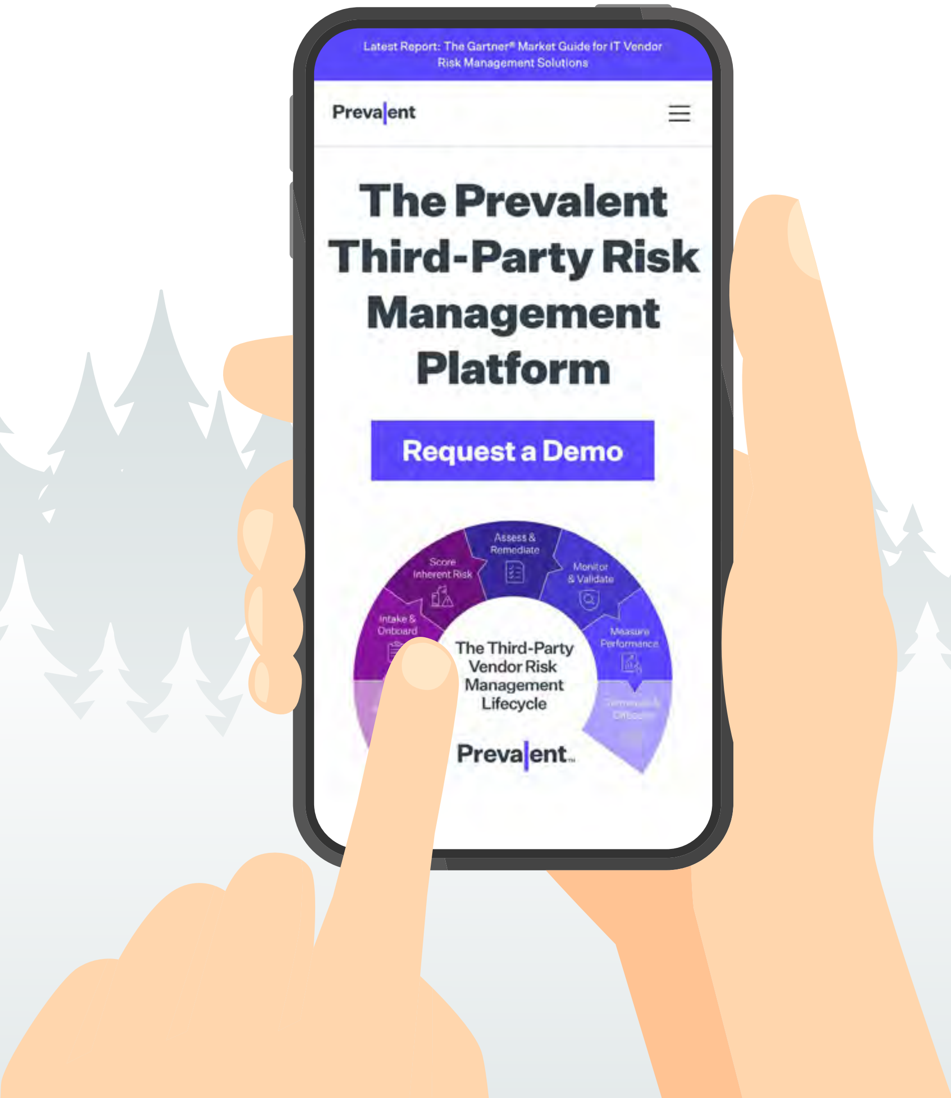
In concert with managed services, investigate the use of AI to speed up reporting, questionnaire completion, and collate data from multiple sources. When considering AI ensure:

- Chosen AI models are trained on years of real third-party risk management expertise, data, and events
- Consideration is made to security, accuracy, and governance of processes and data
- Data is anonymized to reduce the likelihood of a data breach or exposure of personal data

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors and suppliers throughout the third-party lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net.



Latest Report: The Gartner® Market Guide for IT Vendor Risk Management Solutions

Prevalent

The Prevalent Third-Party Risk Management Platform

Request a Demo

Prevalent™