Prevalent™

The 2024 Prevalent

Third-Party Risk Management Study

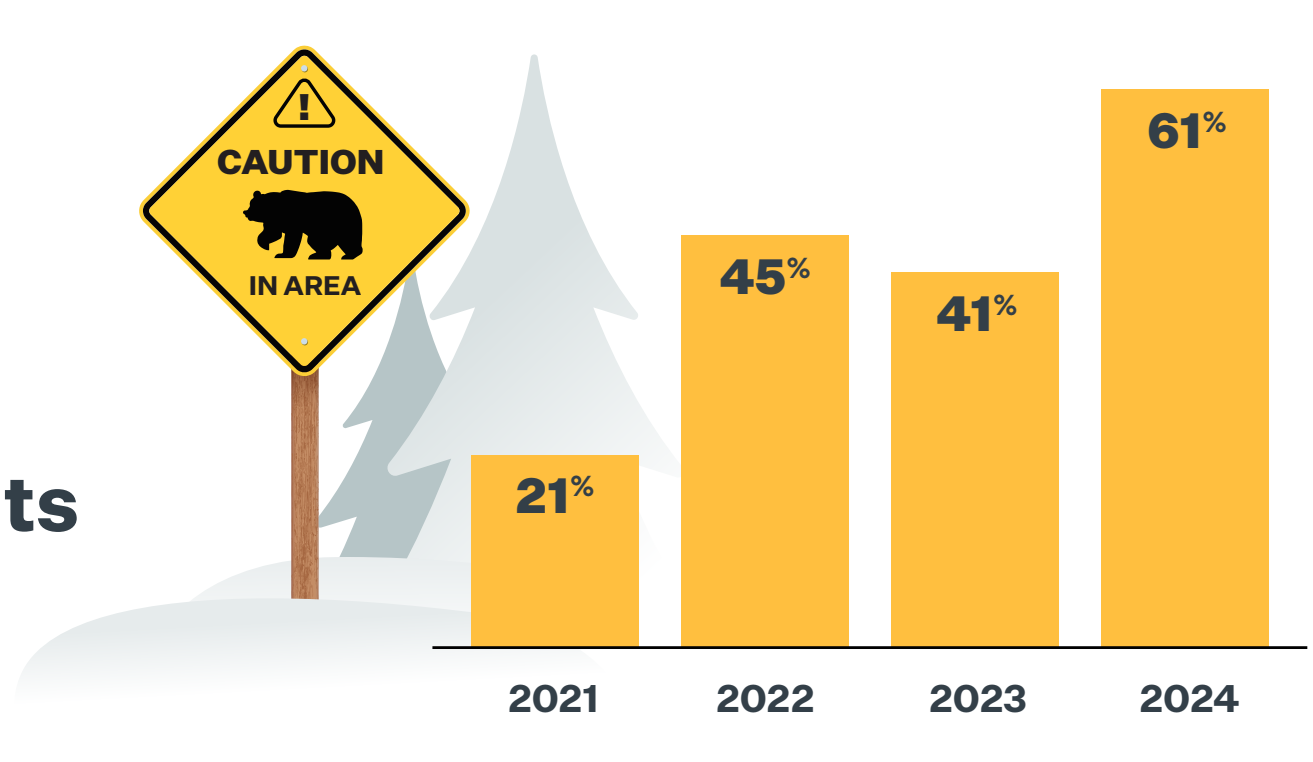
Some TPRM programs are still missing the forest for the trees.

In early 2024, Prevalent conducted a study of trends, challenges, and initiatives impacting third-party risk management (TPRM) practitioners worldwide. The results indicate that many TPRM programs "miss the forest for the trees," as they struggle to meet the broad needs of different stakeholders, sufficiently cover large vendor ecosystems, and address risk at every stage of the third-party lifecycle.

49%
YOY Increase

A Record Level of Third-Party Incidents

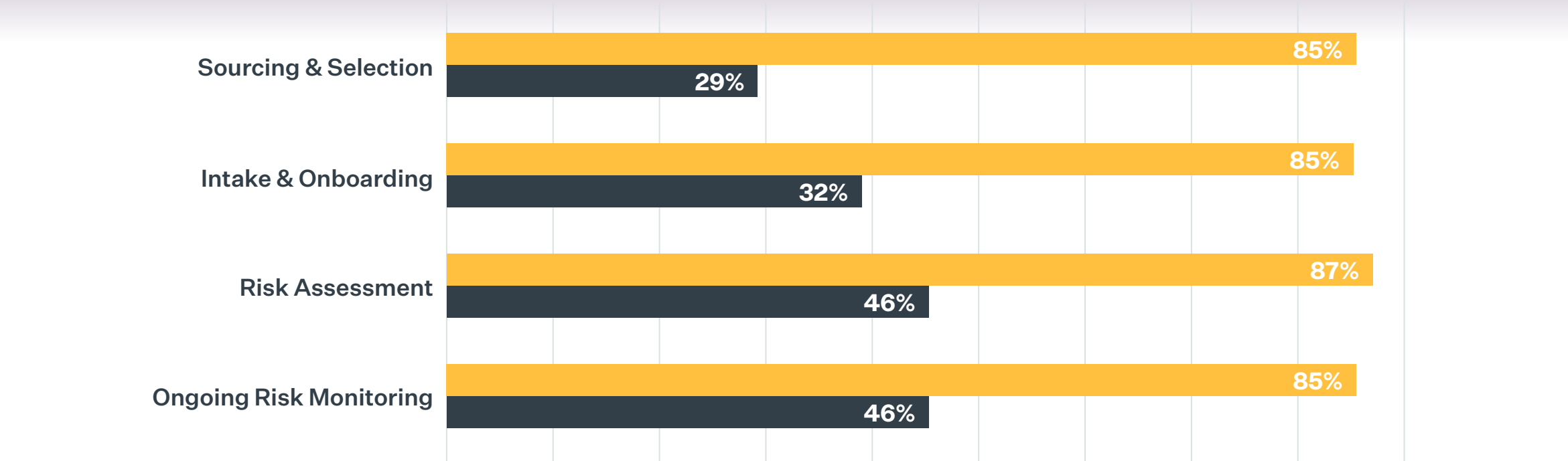
Third-party data breaches are up 49% year over year, with 61% of companies reporting a breach in the last year.



	Tracking More vs. Last Year	Tracking the Same vs. Last Year	Tracking Less vs. Last Year	Not Tracking
Cybersecurity	58%	35%	2%	4%
Data Privacy	39%	55%	3%	3%
Software Supply Chain Security	35%	50%	1%	14%
Compliance (e.g., sanctions)	32%	60%	3%	5%
Business/Operational Resilience	29%	56%	4%	11%
ESG	26%	38%	5%	32%
Financial	18%	64%	4%	14%
Reputational	19%	60%	4%	17%

Some Risks Get More Attention Than Others

Those third-party breaches drove greater involvement in third-party risk. So much so that 58% of orgs are now tracking third-party cybersecurity risks more than last year – more than any other risk type.



Risk Tracking vs. Remediation Across the Vendor Lifecycle

One of the reasons behind the increase in third-party breaches might be the lack of risk remediation at key stages of the third-party lifecycle – especially during Sourcing and Selection and Risk Assessment. You can track risks all you want but, if you don't do something about them, then you could end up with a breach on your hands.

	Currently Tracking Risks	Currently Remediating Risks
Sourcing & Selection	85%	29%
Intake & Onboarding	85%	32%
Risk Assessment	87%	46%
Ongoing Risk Monitoring	85%	46%
Contractual/SLA Performance Monitoring	79%	48%
Offboarding & Termination	74%	44%

Spreadsheets Are Still Popular ...

Complicating the fight against third-party breaches is that organizations are using multiple, sometimes overlapping, tools for TPRM. And it's still a largely manual process, with 50% of companies relying on spreadsheets.

How do you currently assess your third parties?

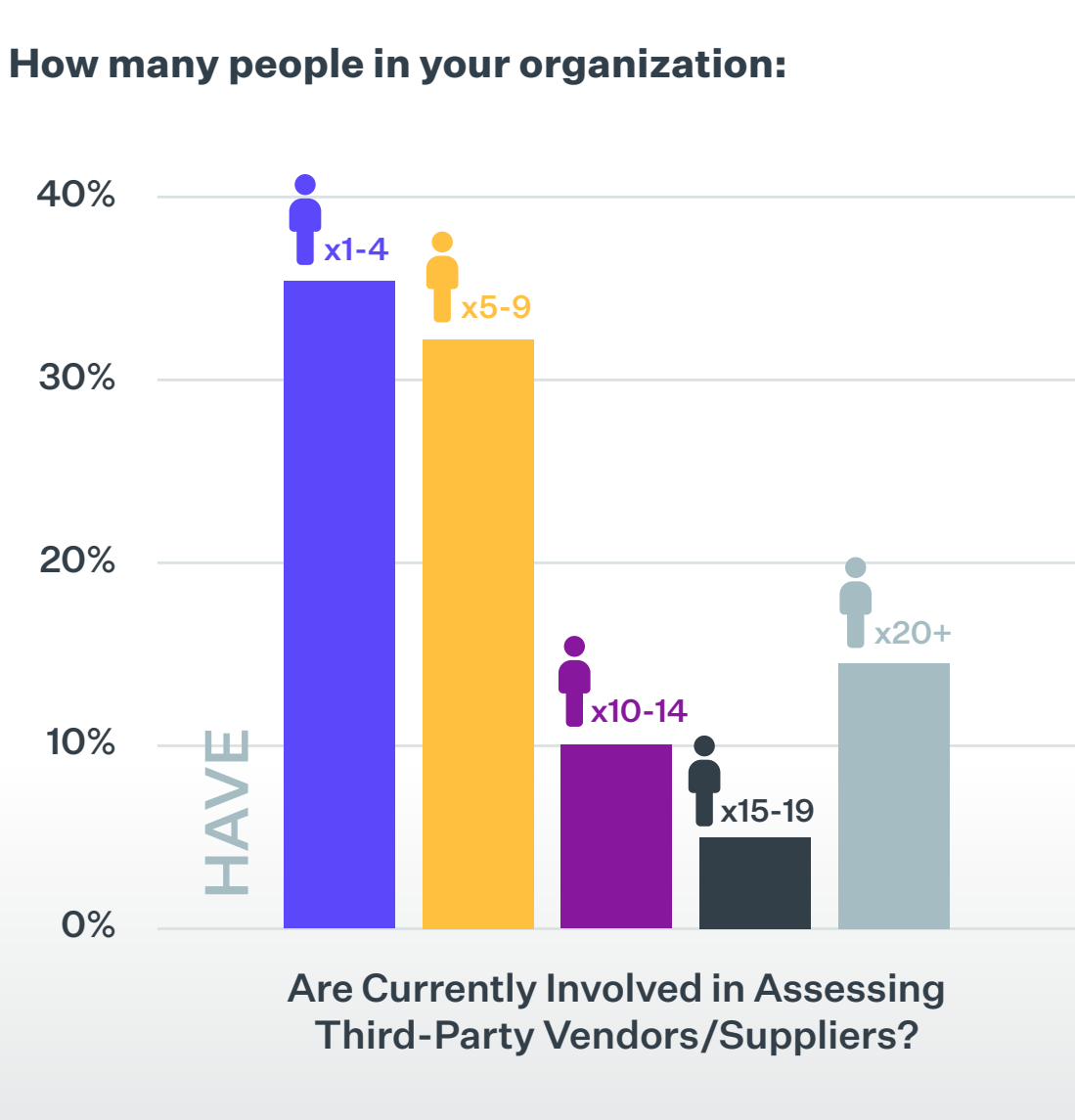
... and Internal Assessments Are Lagging Behind External Monitoring

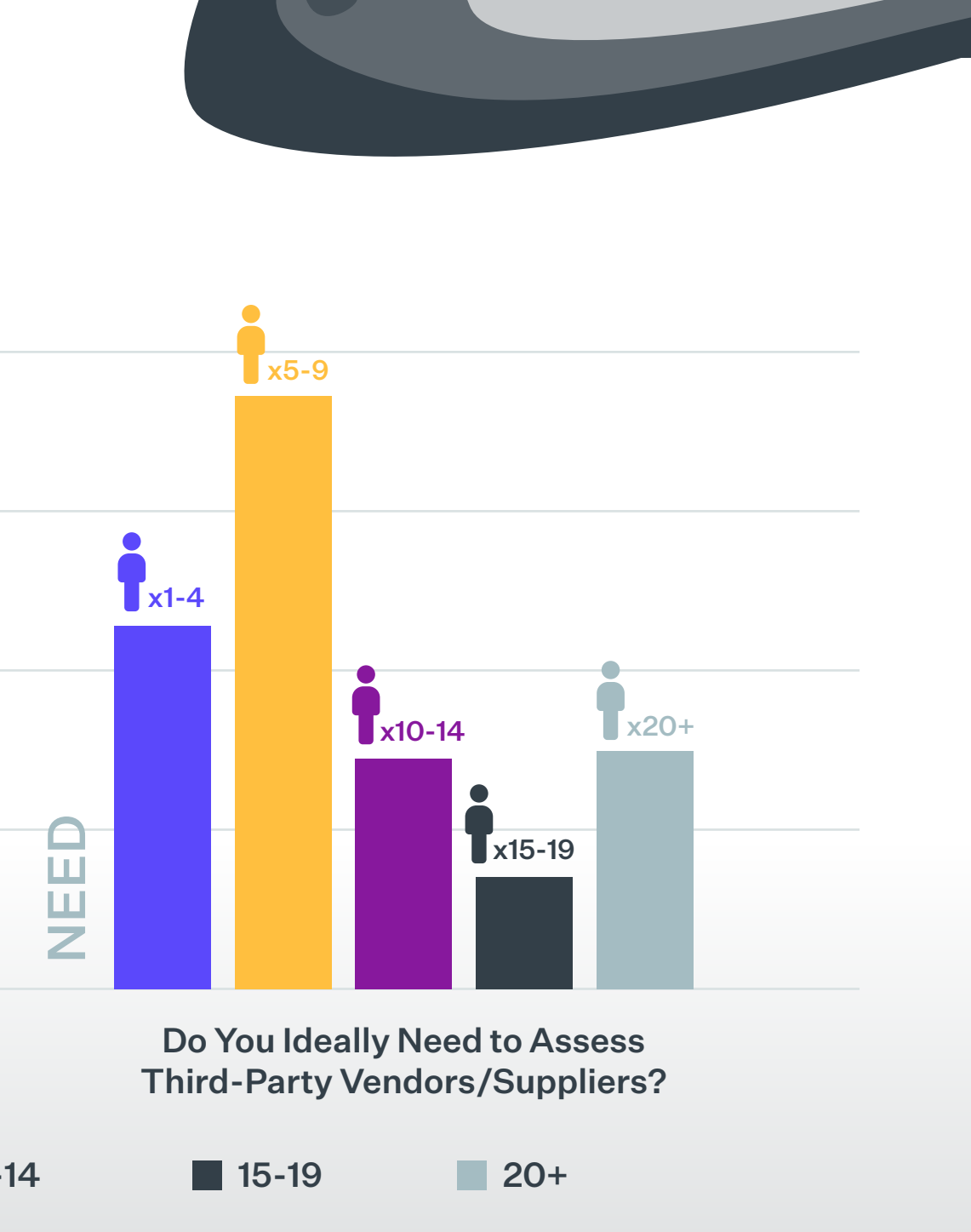
Given the increase in breaches, it's not surprising that companies are using security ratings services more vs. last year. But the concerning trend is that companies are monitoring cyber risks more than they are assessing cyber risks. The downfall is that monitoring provides no view of internal controls.

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

Understaffed Teams Are Managing Only 33% of Vendors

With all those breaches to manage, infosec teams are overwhelmed – so much so that they're only managing a third of vendors due to understaffing by a factor of two!

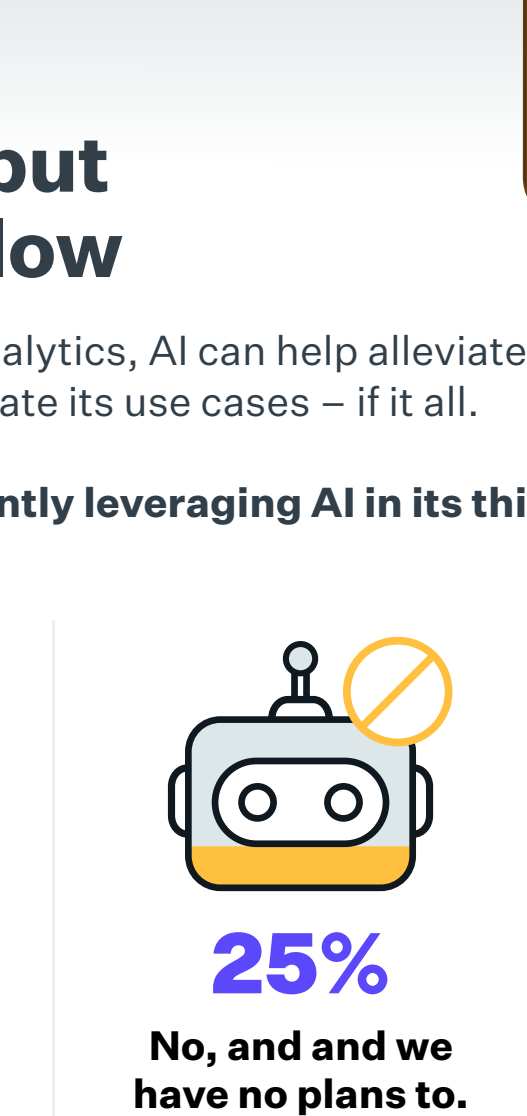




How many people in your organization:

Barriers to TPRM Growth

In fact, companies say a lack of resources is the number one barrier to growing their TPRM programs.



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

AI May Help, but Adoption Is Slow

With its automations and analytics, AI can help alleviate resourcing concerns. But for most companies they're only just starting to investigate its use cases – if it all.

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.

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

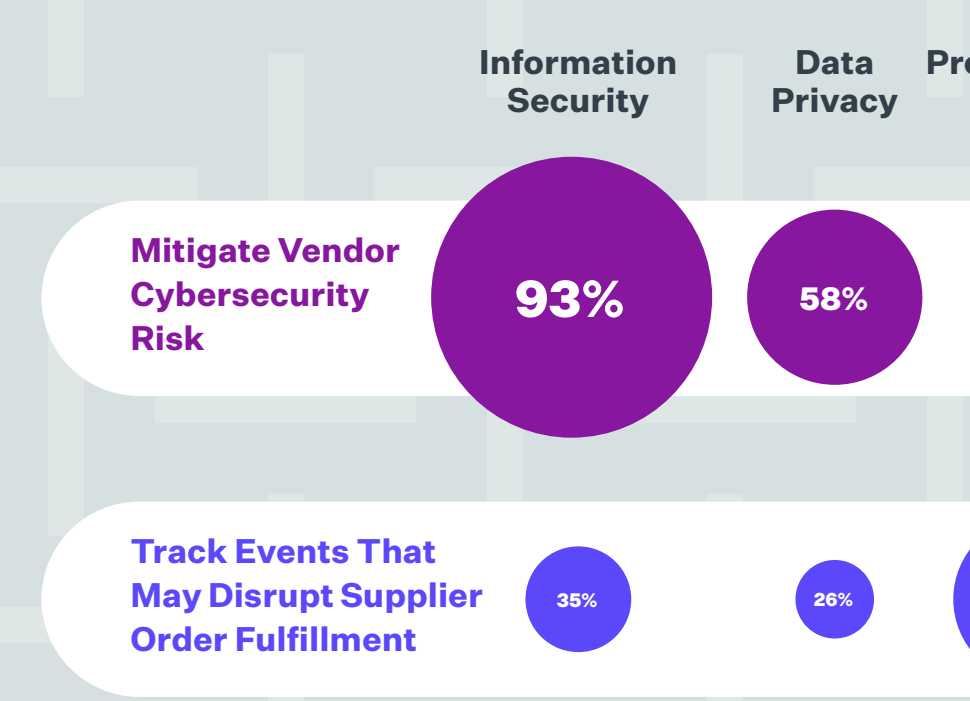
- **58%** **Extracting more valuable insights** from data for reporting
- **54%** **Speeding up questionnaire completion** by automatically populating surveys using existing questionnaires and available evidence
- **54%** **Collating and centralizing data from multiple sources** for more comprehensive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

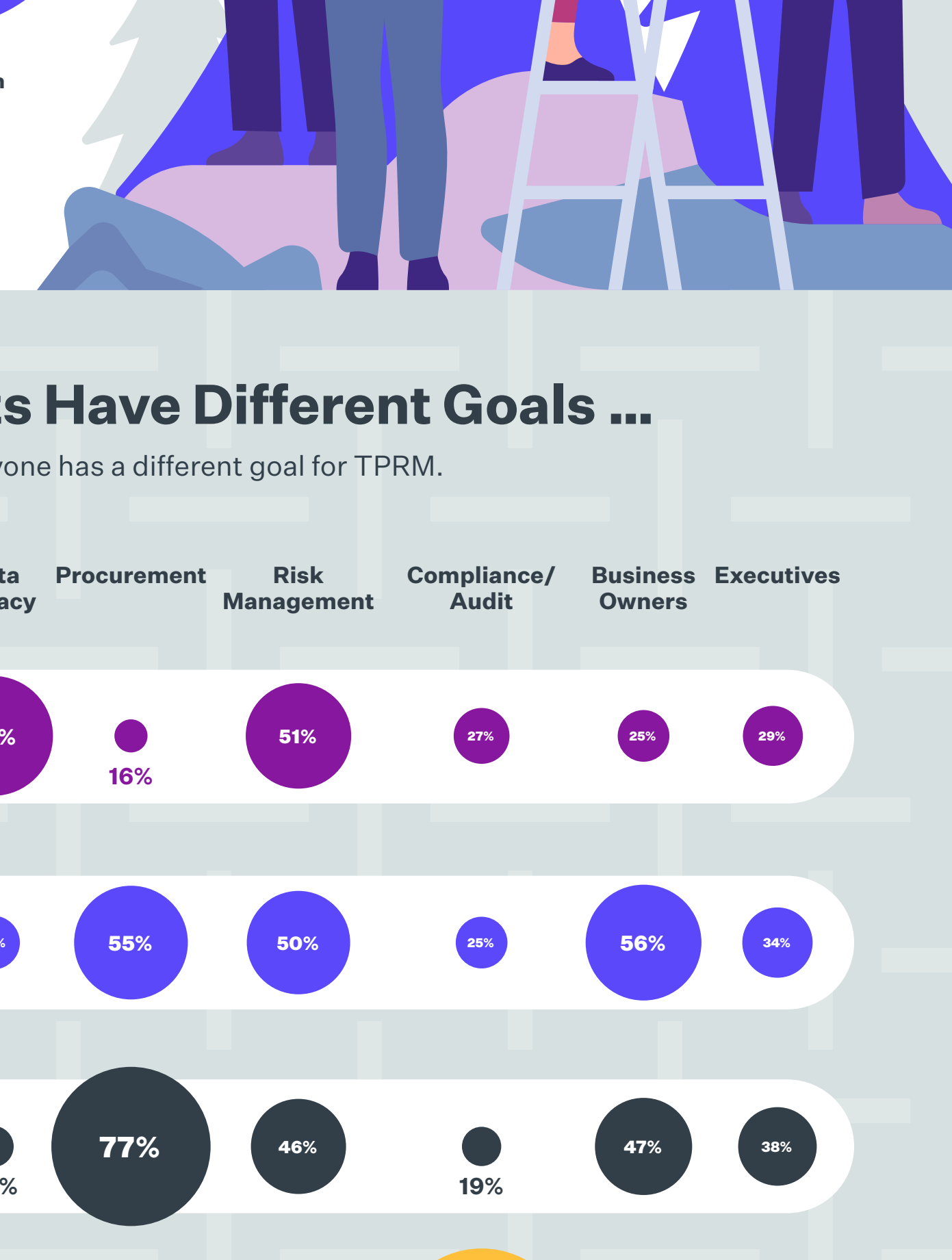
Why do you have no plans to use AI in your TPRM program?

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

Coordination Needs Improvement

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.





Different Departments Have Different Goals ...

Coordination can be challenging when everyone has a different goal for TPRM.

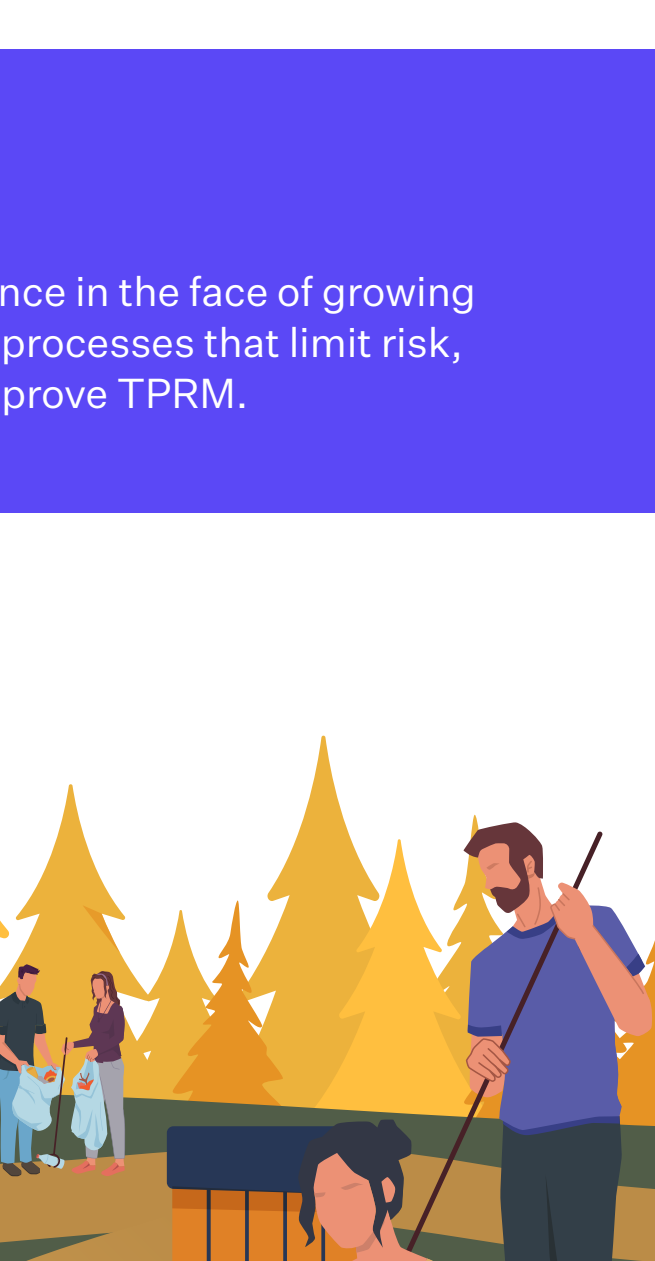
	Information Security	Data Privacy	Procurement	Risk Management	Compliance/ Audit	Business Owners	Executives
Mitigate Vendor Cybersecurity Risk	93%	58%	16%	51%	27%	25%	29%
Track Events That May Disrupt Supplier Order Fulfillment	35%	26%	55%	50%	25%	56%	34%
Speed And/Or Simplify New Vendor/Supplier Onboarding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

... And Own Different Pieces of the Third-Party Management

And there's a pretty complex ownership arrangement between Information Security, Business Owners, and Procurement in place in most companies.

In your organization, which department primarily:

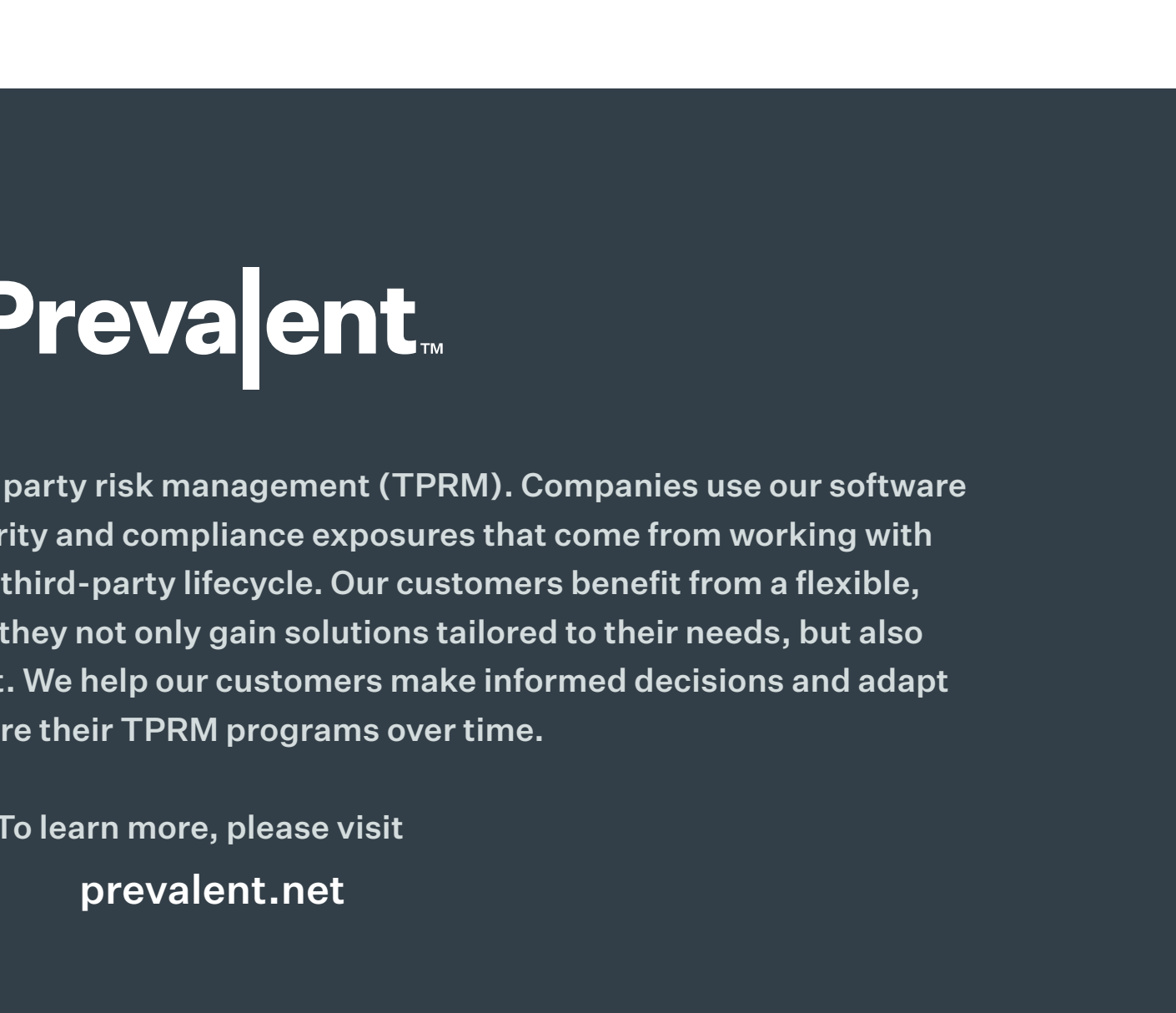
	Owns the TPRM Program	Owns the Third-Party Relationship	Manages the Third-Party Database
1	Information Security	Business Owners	Procurement
2	Risk Management	Procurement	Information Security
3	Compliance/Audit	Information Security	Risk Management
4	Procurement	Compliance/Audit	Compliance/Audit
5	Data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



Recommendations

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**
- **Automate TPRM processes around a single platform to unify teams, data, and the risk lifecycle**
- **Close the resource and skill gap with outsourced managed services or artificial intelligence capabilities**



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 across 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. We help our customers make informed decisions and adapt and mature their TPRM programs over time.

To learn more, please visit

prevalent.net