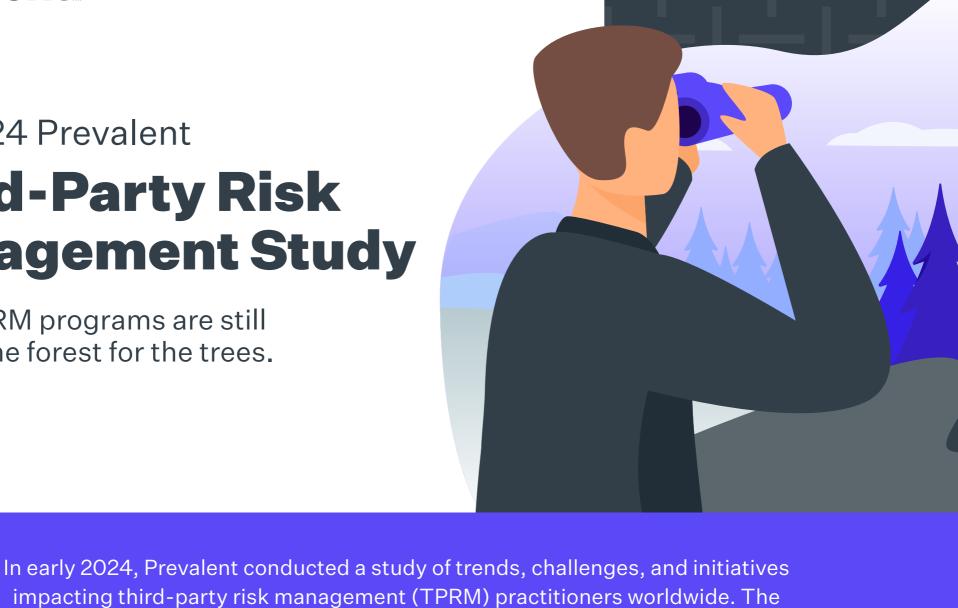
## Preva ent<sub>™</sub> The 2024 Prevalent **Third-Party Risk**

## **Management Study** Some TPRM programs are still

missing the forest for the trees.

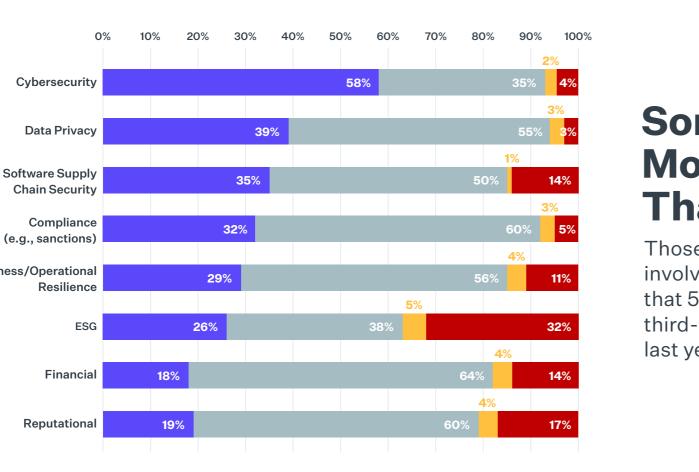


results indicate that many TPRM programs "miss the forest for the trees," as they struggle to meet the broad needs of different stakeholders, sufficiently cover large vendor ecosystems, and address risk at every stage of the third-party lifecycle. 49%

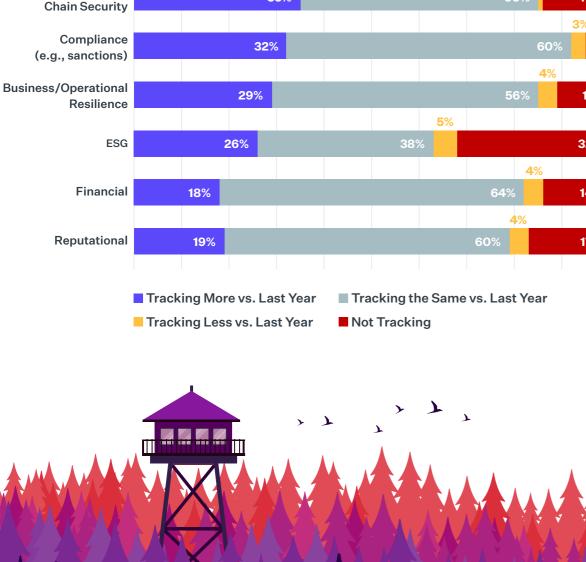


### year over year, with 61% of companies reporting a breach in the last year.

Cybersecurity **Data Privacy** 



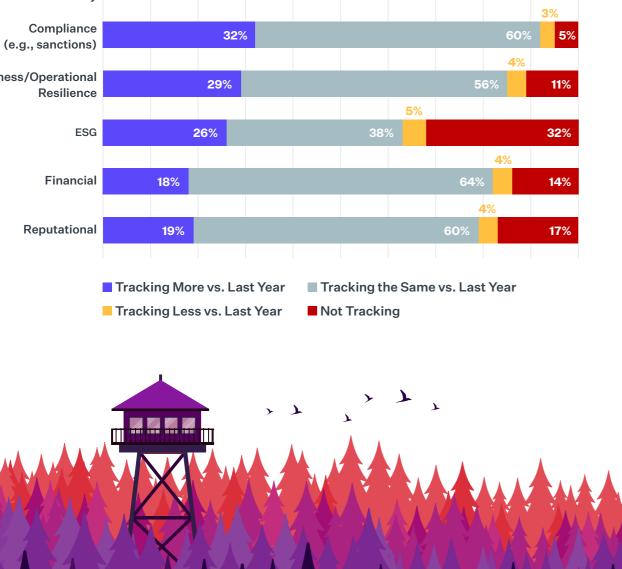




# that 58% of orgs are now tracking

involvement in third-party risk. So much so third-party cybersecurity risks more than last year – more than any other risk type.

61%



#### 0% 10% 20% 30% 40% **Sourcing & Selection** 29% Intake & Onboarding 32%

**Risk Assessment** 

**Ongoing Risk Monitoring** 

25%

20%

15%

0%

80%

70%

60%

50%

40%

30%

20%

10%

20%

10%

0%

2021

**Risk Tracking vs. Remediation** 

**Across the Vendor Lifecycle** 

Spreadsheets Are Still Popular ... Complicating the fight against third-party breaches is that organizations are using multiple, sometimes

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

50%

46%

46%

**Procurement Systems\*** 

Other\*

2024

(T)

**Privacy Management Tool\*** 

**Don't Assess Third Parties** 

**Supply Chain Management Tool\*** 

Risk Exchange Networks/Marketplaces\*

60%

70%

80%

85%

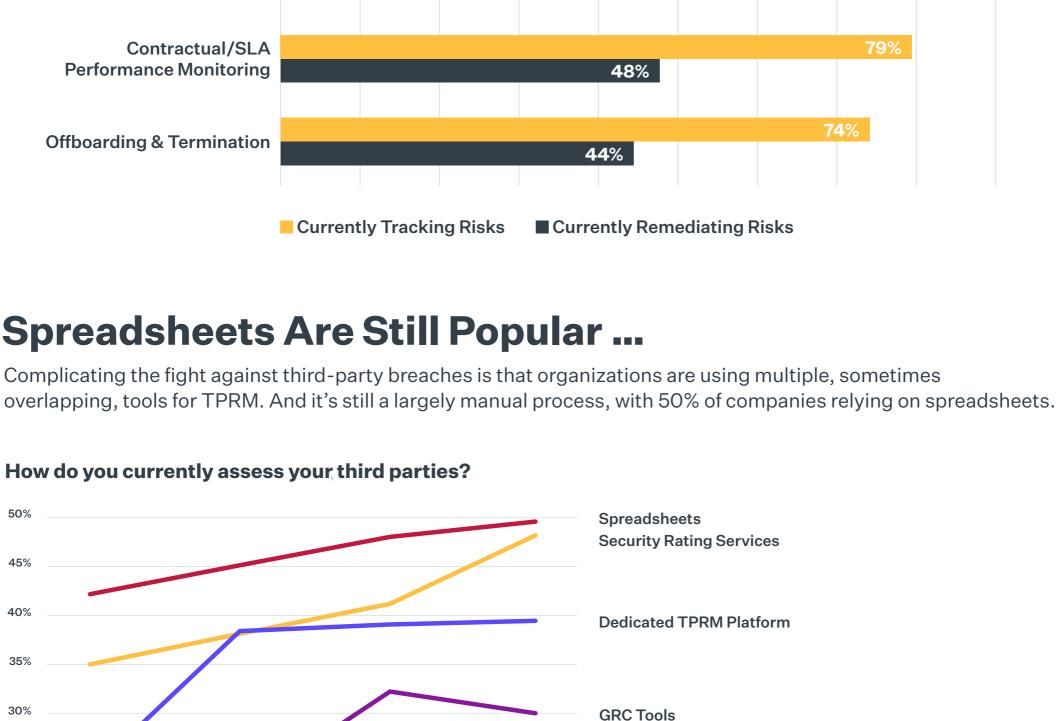
85%

87%

85%

90%

all you want but, if you don't do something about them, then you could end up with a breach on your hands.



#### 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.

(T

 $\mathcal{O}_{j}$ 

Given the increase in breaches, it's not surprising that

2022

**Are Lagging Behind** 

**External Monitoring** 

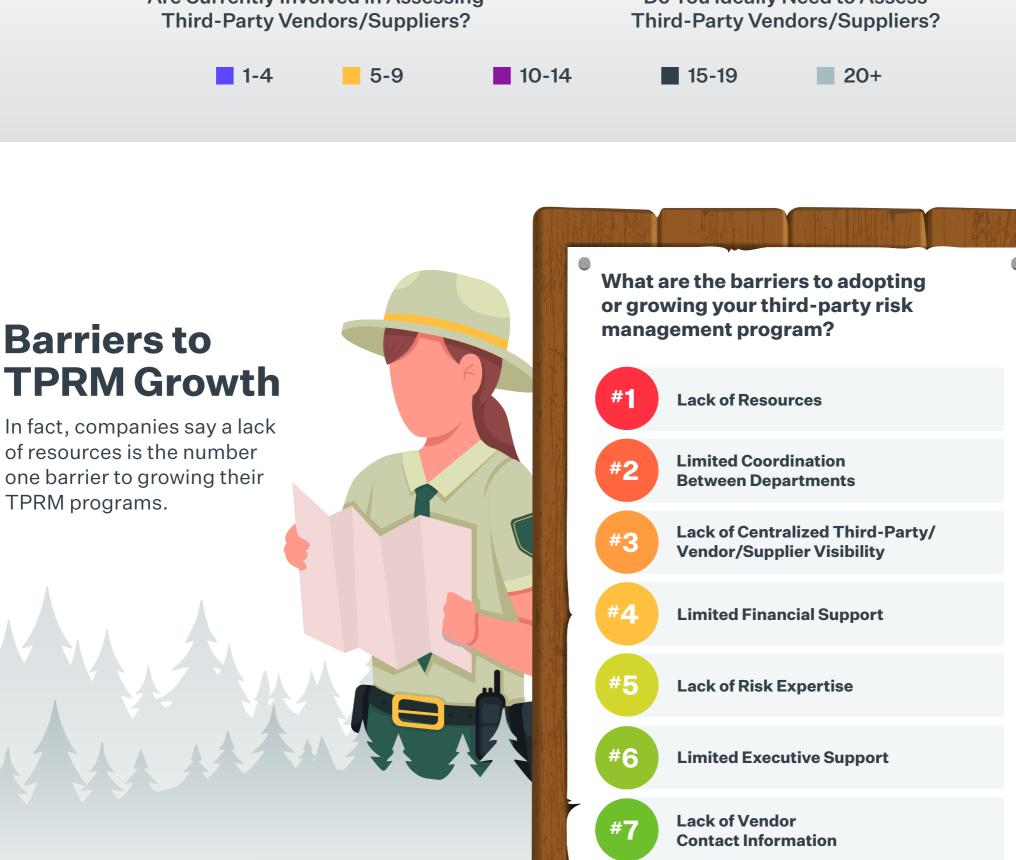
2023

0% **ESG** Cybersecurity Software Supply **Data Privacy** Compliance **Chain Security** (e.g., sanctions)









#### **Extracting more valuable insights** from data for reporting **54% Speeding up questionnaire** completion by automatically

**54**%

38%

Coordination

Al May Help, but

**Adoption Is Slow** 

61%

No, but we are

investigating

its use cases.

**TPRM program?** 

only just starting to investigate its use cases – if it all.

What are your goals with using

or investigating Al for use in your

populating surveys using existing

questionnaires and available evidence

Collating and centralizing data from

comprehensive vendor due diligence

multiple sources for more

**Getting instant risk** 

**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

31%

**Highly** 

Coordinated

remediation guidance

**25%** 

No, and and we

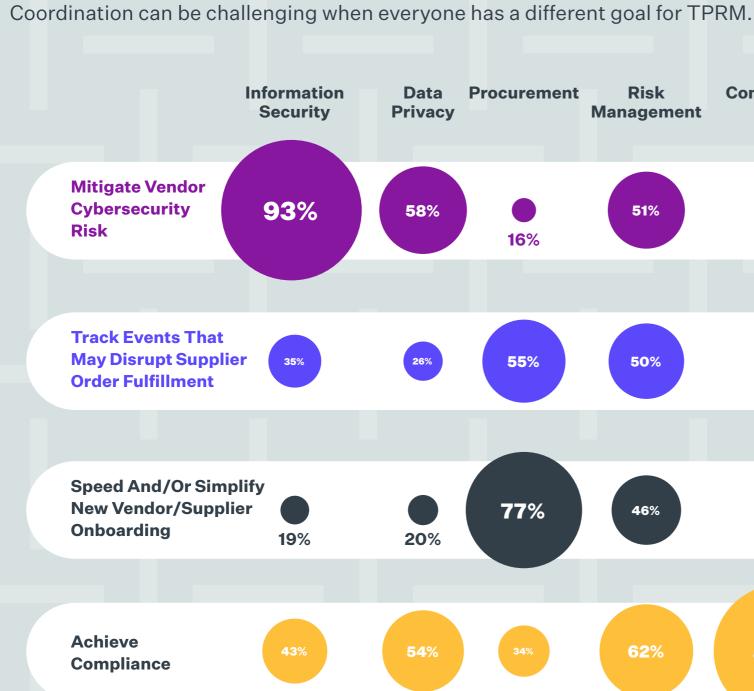
have no plans to.

organization, with a surprisingly small 31% of respondents indicating a highly coordinated program.

**51%** 

Some

Coordination



And there's a pretty complex ownership arrangement between Information Security, Business Owners, and

In your organization, which department primarily:

Owns the

**Third-Party Relationship** 

**Business Owners** 

**Procurement** 

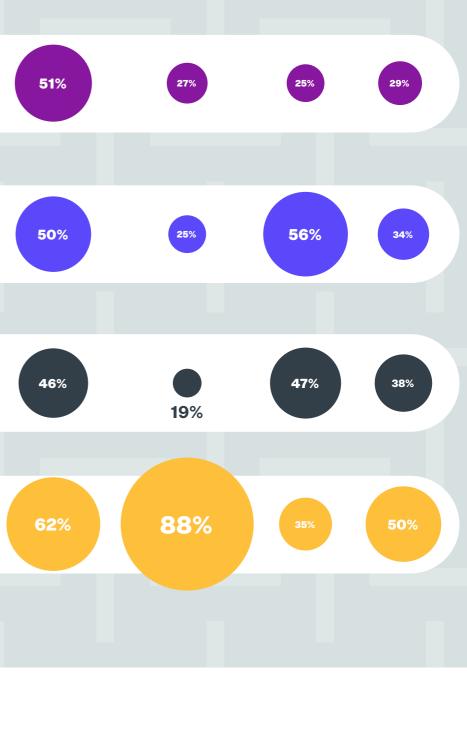
Procurement in place in most companies.

**Owns the TPRM Program** 

(2)

**Information Security** 

**Risk Management** 



risk lifecycle Close the resource and skill

**Download the Study** Preva ent...

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

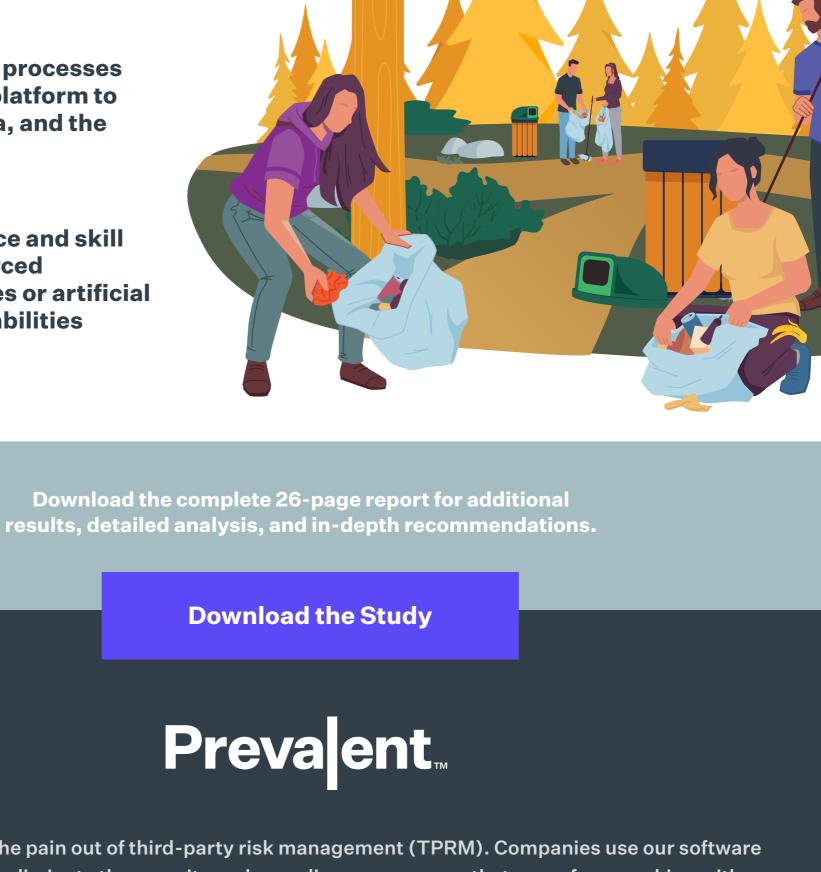
© Prevalent, Inc. All rights reserved. The Prevalent name and logo are trademarks or registered trademarks of Prevalent, Inc. All other trademarks are the property of their respective owners. 04/24

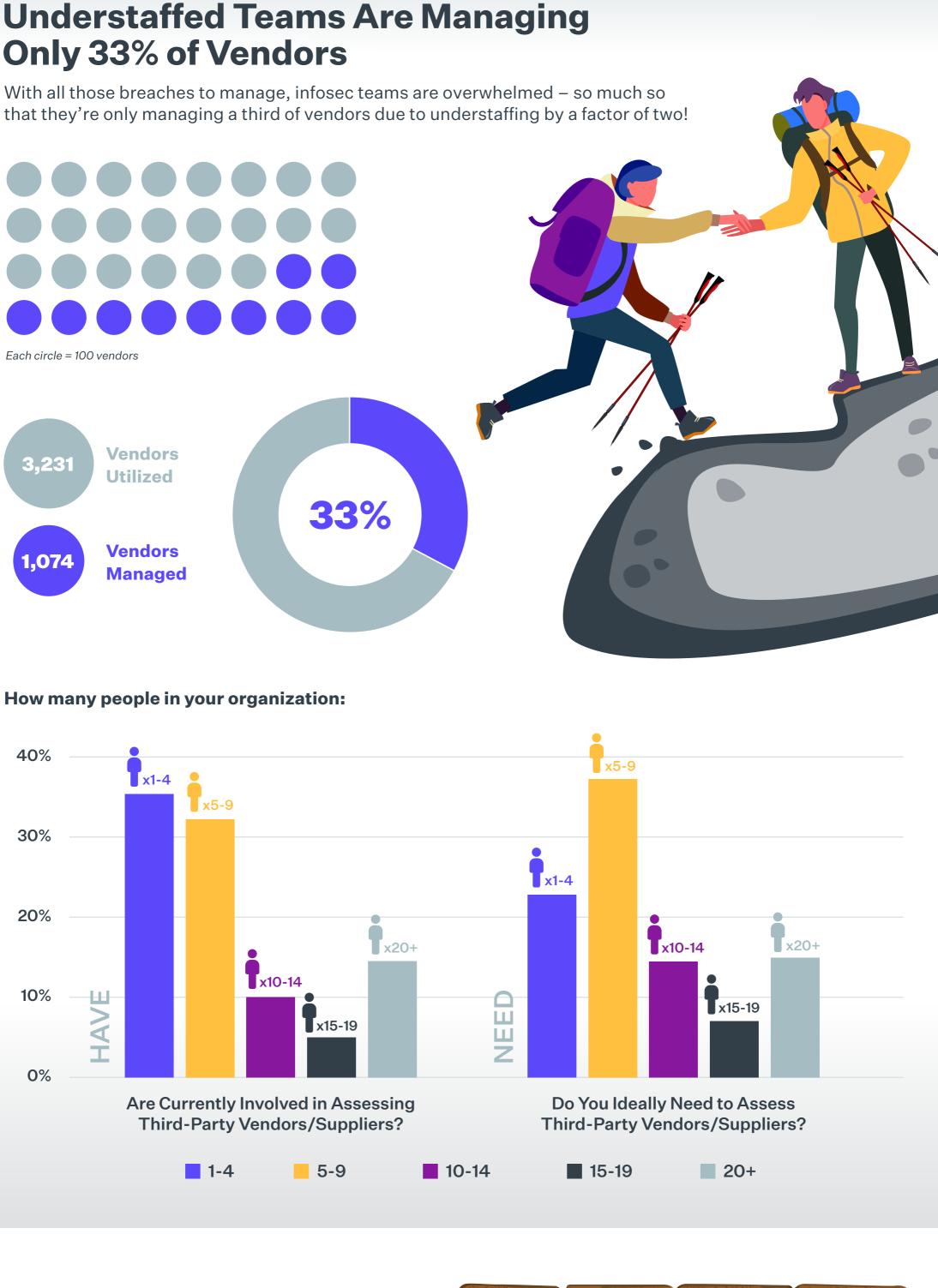
prevalent.net

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

Compliance/Audit **Information Security**  $\left(4\right)$ Compliance/Audit **Procurement Risk Management Data Privacy Executives Executives Business Owners Data Privacy** 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 gap with outsourced managed services or artificial intelligence capabilities





With its automations and analytics, Al can help alleviate resourcing concerns. But for most companies they're Is your organization currently leveraging AI in its third-party risk management program? 5% Don't know Yes, we are actively using Al in our **TPRM** program.

Why do you have no plans to use

Al in your TPRM program?

49% No organizational strategy for Al

**Data security risks** 

algorithm models

9% Risks of bias or hallucination

Lack of transparency in

Different Departments Have Different Goals ... Compliance/ **Business Executives** Risk Management **Audit Owners** 

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

Manages the

**Third-Party Database** 

**Information Security** 

**Risk Management** 

Compliance/Audit

**Business Owners** 

**Data Privacy** 

**Executives** 

**Procurement**