Prevalent™

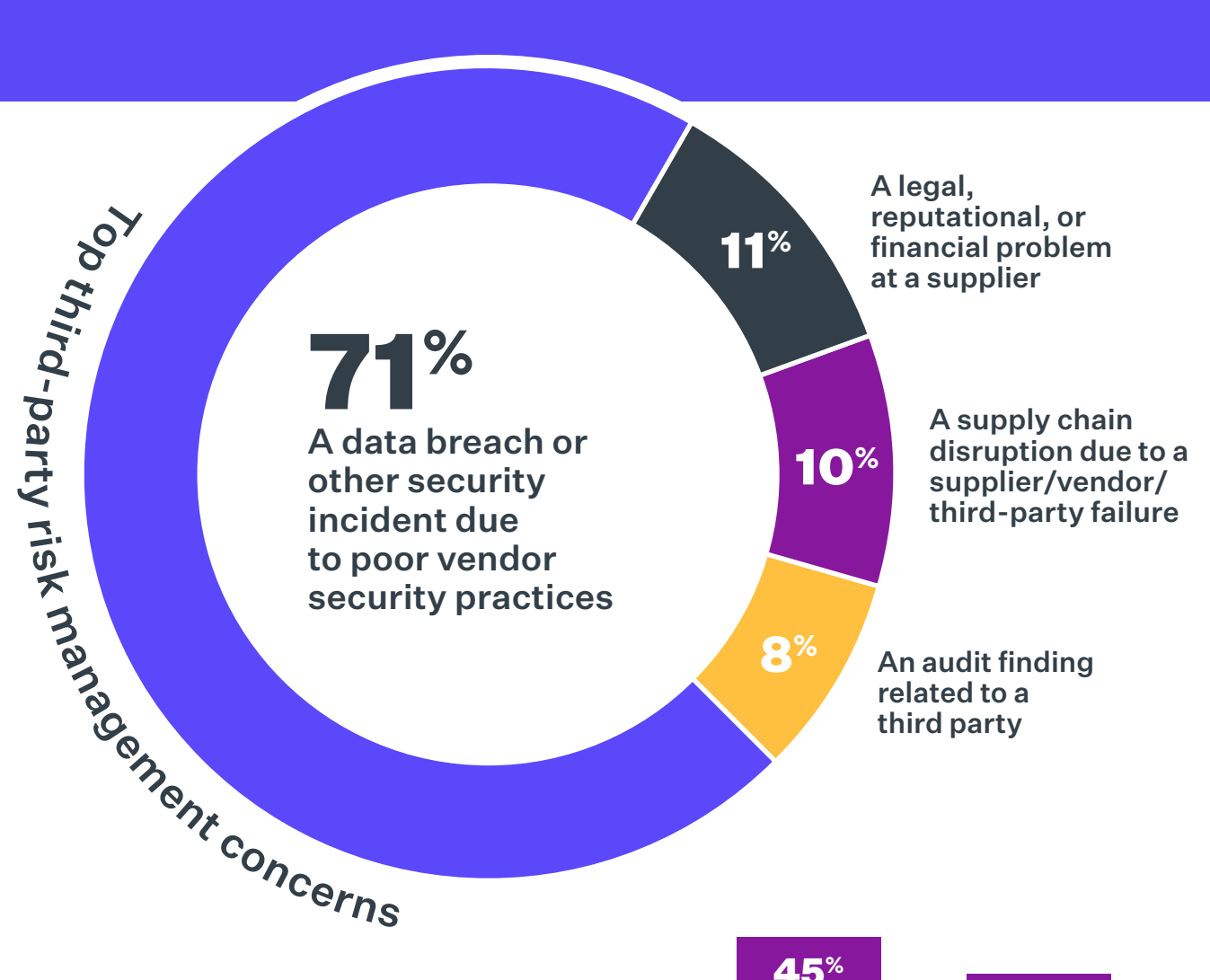
The 2023 Prevalent Third-Party Risk Management Study

How Are Organizations Avoiding TPRM Turbulence?

In early 2023, Prevalent conducted a study on current trends, challenges and initiatives impacting third-party risk management (TPRM) practitioners worldwide– specifically as they relate to the use of **manual processes, third-party incident response and the vendor lifecycle.**

Top Concern: Data Breaches

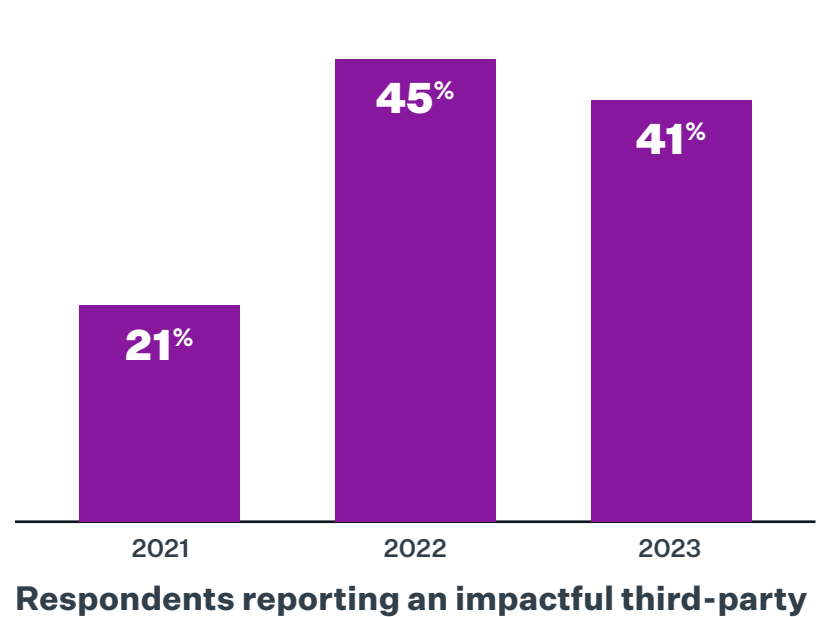
Companies reported that the top concern regarding their usage of third parties was a data breach or other security incident due to poor vendor security practices.



Primary Impact: Cost

41% of respondents reported experiencing a data breach or other security incident that had a tangible impact in the last 12 months.

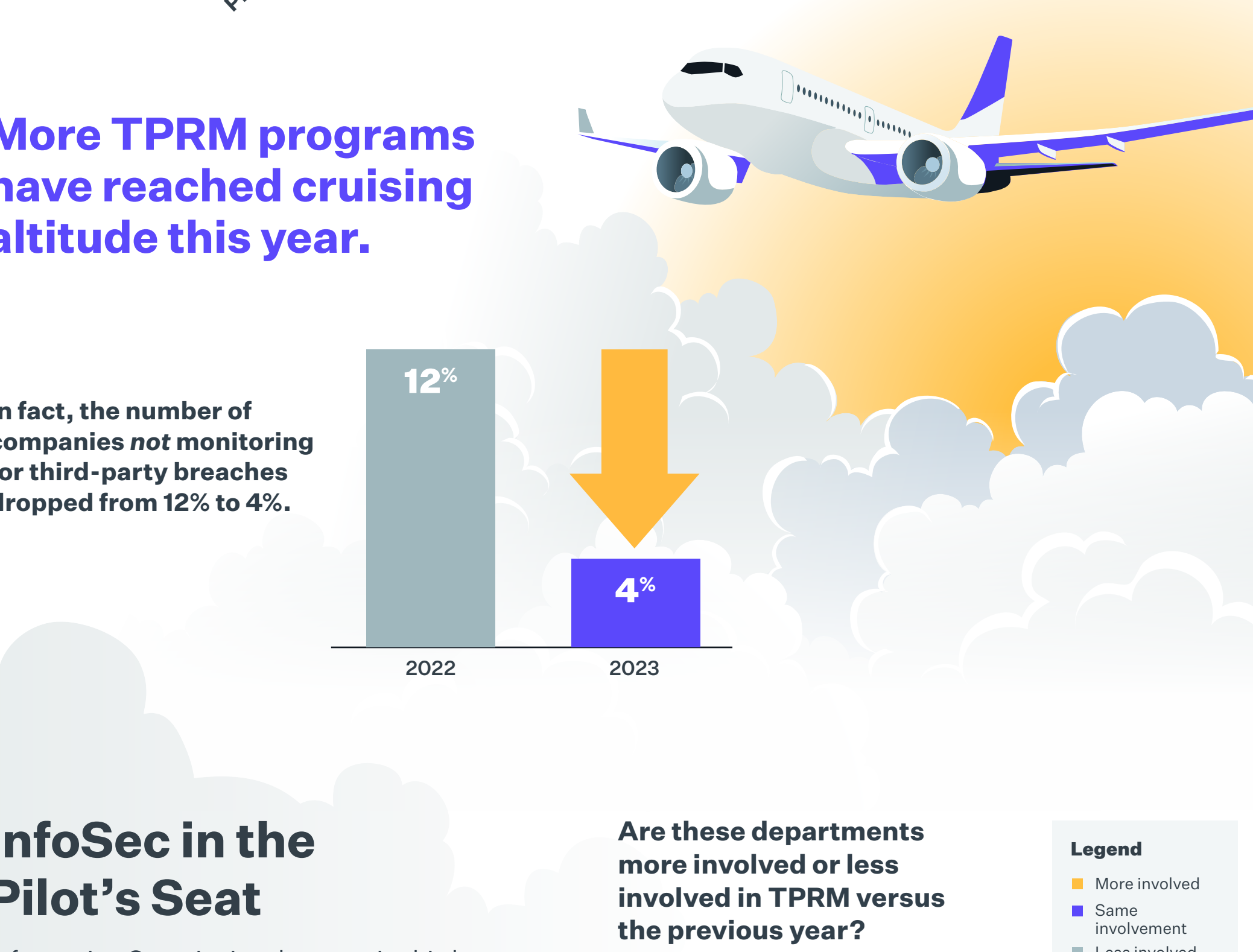
Those incidents primarily resulted in **costs to remediate or recover** from the breach or incident — more so than losing customers, revenue or reputation.

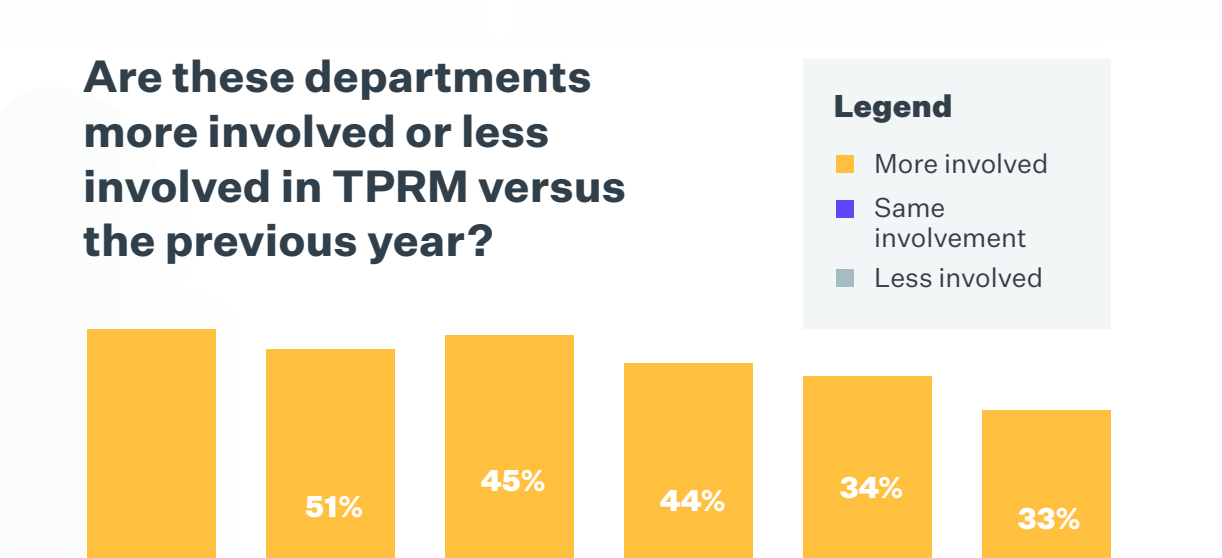


Respondents reporting an impactful third-party security incident in the last 12 months

More Tools Available

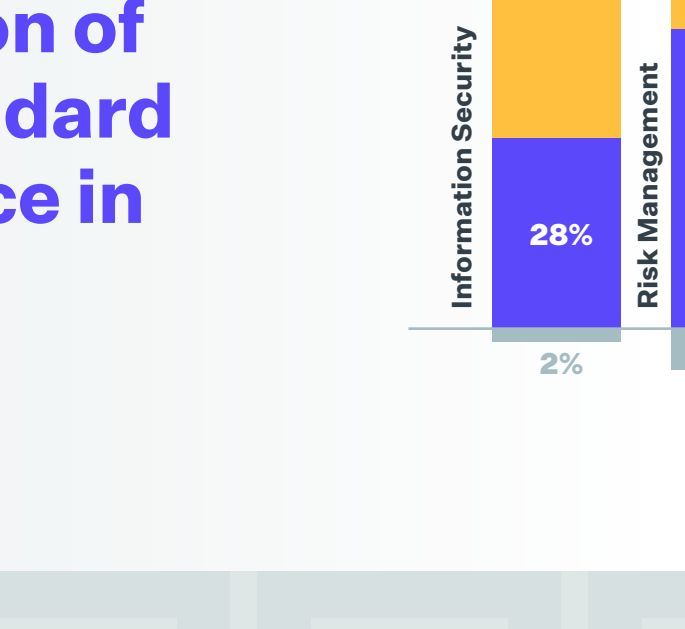
Organizations reported having access to more response tools, such as Dark Web monitoring and data breach monitoring, versus in the previous year. This may be why the number of third-party incidents appears to have leveled off. The downside? Way too many companies are manually assessing vendors.





More TPRM programs have reached cruising altitude this year.

In fact, the number of companies *not* monitoring for third-party breaches dropped from 12% to 4%.

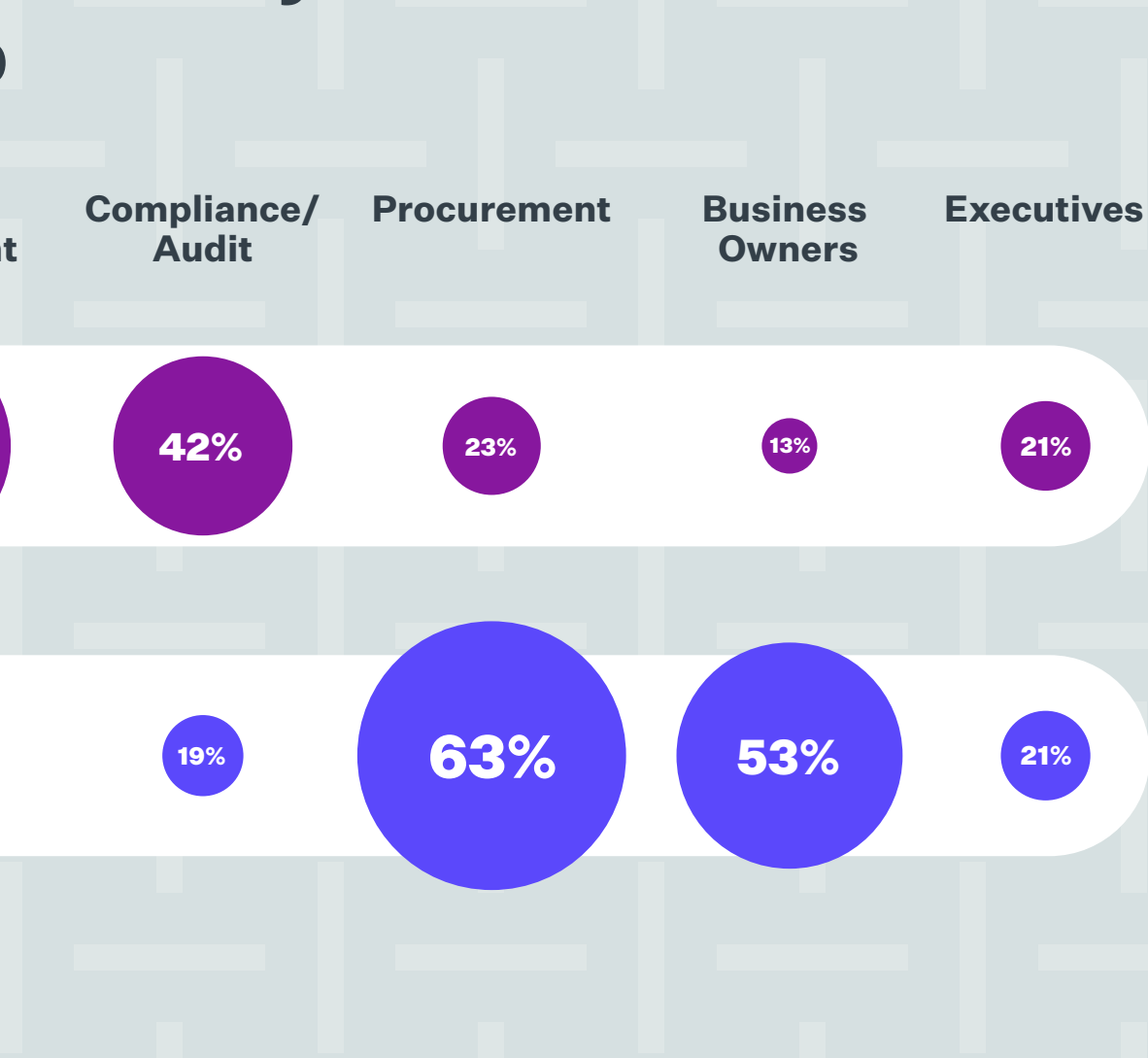


InfoSec in the Pilot's Seat

Information Security involvement in third-party risk management increased for 70% of respondents, and the InfoSec department now owns the TPRM program in 71% of companies.

We believe this signals a greater adoption of TPRM as a standard security practice in organizations.

Are these departments more involved or less involved in TPRM versus the previous year?



TPRM Program and Third-Party Relationship Ownership

	Information Security	Risk Management	Compliance/ Audit	Procurement	Business Owners	Executives
Owns the TPRM Program	71%	53%	42%	23%	13%	21%
Owns the Third-Party Relationship	35%	20%	19%	63%	53%	21%

What's Driving the Increased Involvement?

62% of respondents indicated that third-party data breaches and security incidents were top drivers behind increased Information Security involvement.

62% Third-party data breaches and security incidents

60% Increasing regulatory scrutiny

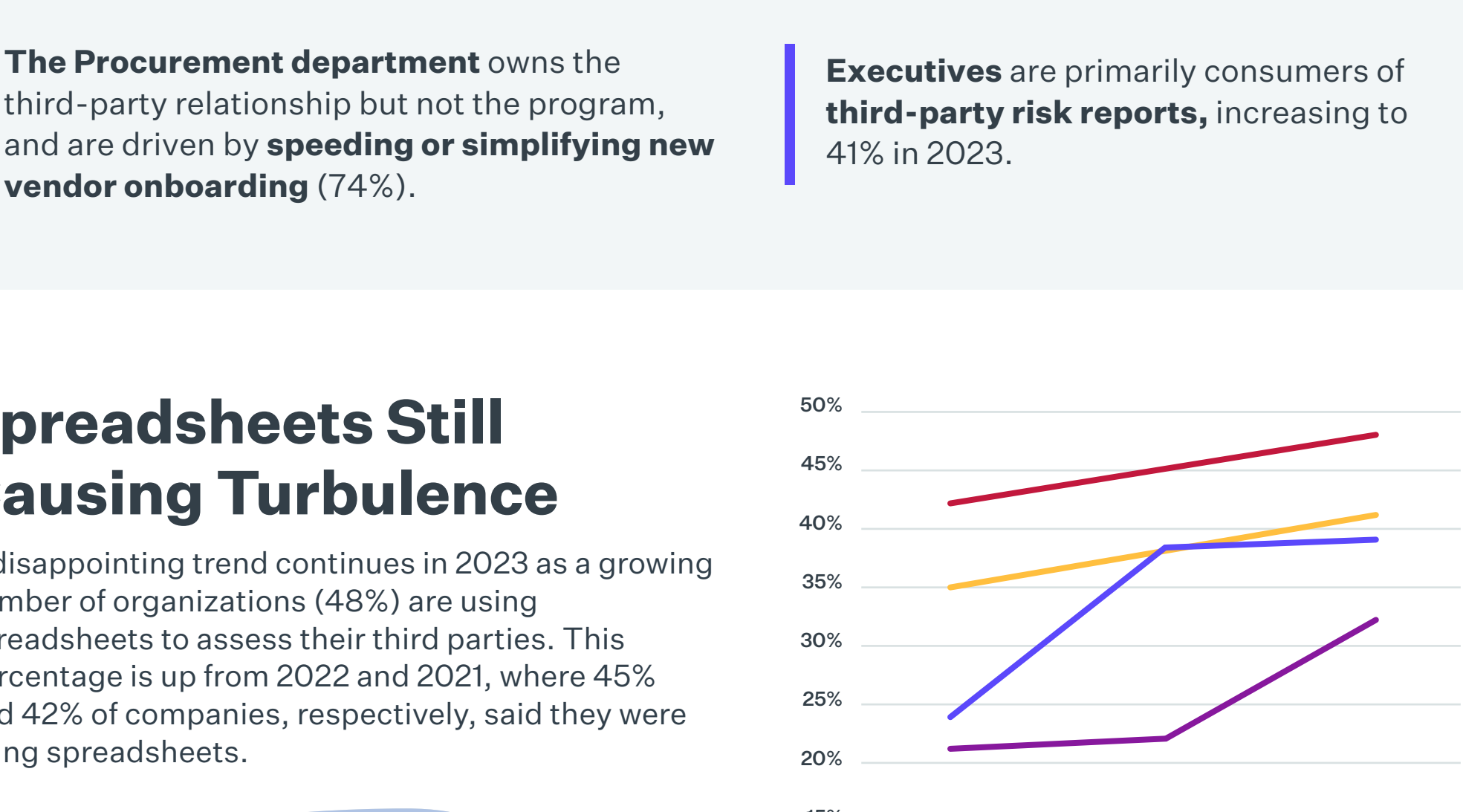
49% Executive visibility

38% Supply chain disruptions

TPRM Remains a Team Effort

TPRM still relies on contributions from several departments with distinct priorities, with all departments increasing their involvement since last year.

Involvement by Department



When we asked about departmental goals for TPRM, we learned:

Risk Management teams want to **achieve compliance** (53%) **and address the risks** of working with IT vendors (52%).

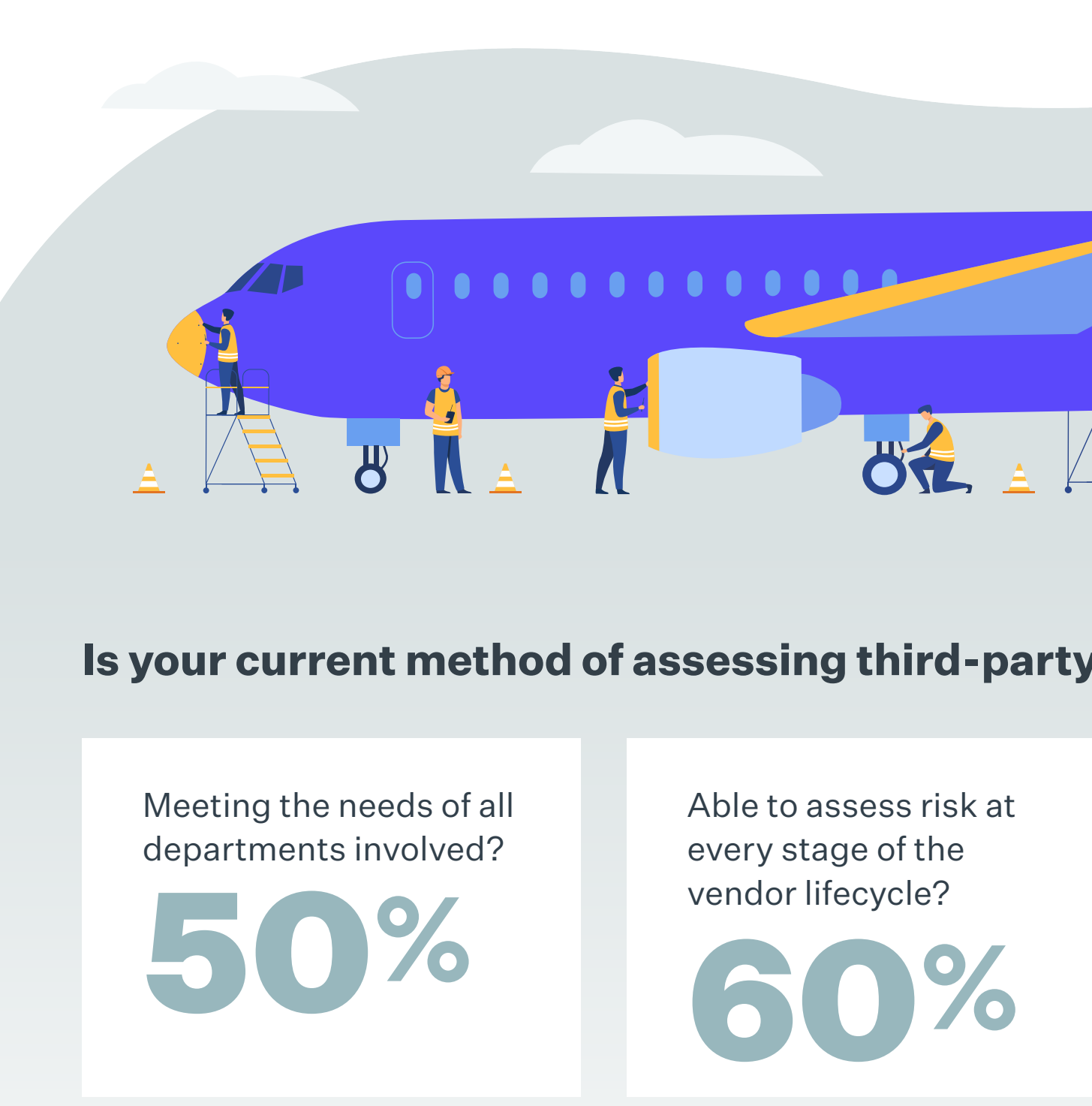
Compliance/Audit teams want to **achieve compliance** (79%), as do Executives (51%) and Business Owners (44%).

The Procurement department owns the third-party relationship but not the program, and are driven by **speeding or simplifying new vendor onboarding** (74%).

Executives are primarily consumers of **third-party risk reports,** increasing to 41% in 2023.

Spreadsheets Still Causing Turbulence

A disappointing trend continues in 2023 as a growing number of organizations (48%) are using spreadsheets to assess their third parties. This percentage is up from 2022 and 2021, where 45% and 42% of companies, respectively, said they were using spreadsheets.



Manual Methods Don't Fly

It therefore shouldn't come as a surprise that a growing percentage of companies responded "Unsure" when asked if their current method of assessing risks throughout the lifecycle, assessing multiple risk types, reporting and incident response was working.

Is your current method of assessing third-party risk...

Meeting the needs of all departments involved? **50%**

Able to assess risk at every stage of the vendor lifecycle? **60%**

Able to assess risks across security, business and reputational categories? **45%**

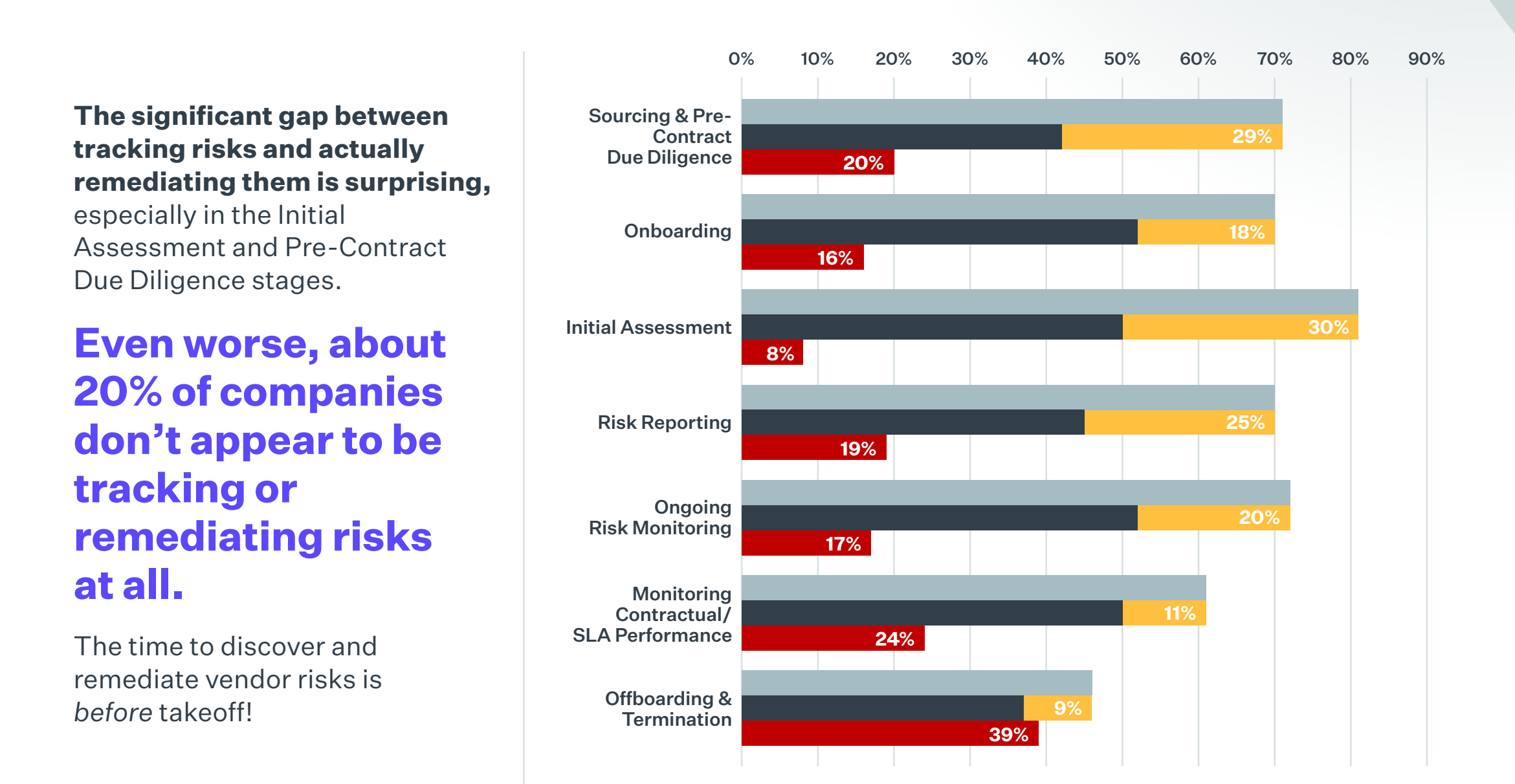
Delivering the automation and reporting necessary to efficiently demonstrate compliance? **62%**

Helping you be more proactive in third-party incident response? **42%**

Satisfying executive and board demands for more information on third-party risks? **43%**

Post-Flight Checks Are Lacking

The **Offboarding and Termination** stage of the third-party relationship lifecycle sees the lowest percentage of companies tracking (47%) and remediating (38%) risks, and the highest percentage of companies doing nothing at all (39%).



47% Tracking Offboarding and Termination

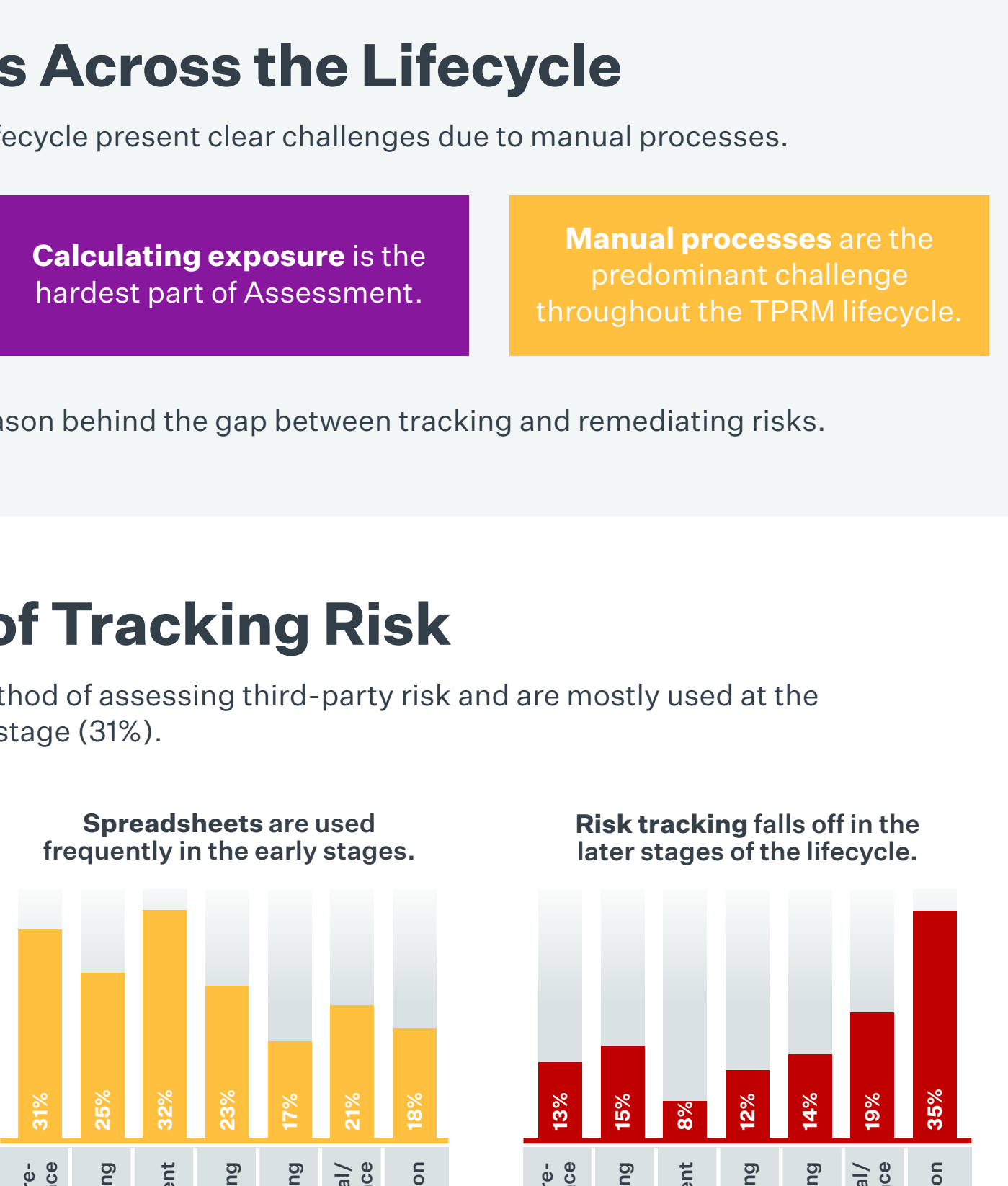
38% Remediating Offboarding and Termination

39% Doing Nothing During Offboarding and Termination

The significant gap between tracking risks and actually remediating them is surprising, especially in the Initial Assessment and Pre-Contract Due Diligence stages.

Even worse, about 20% of companies don't appear to be tracking or remediating risks at all.

The time to discover and remediate vendor risks is *before* takeoff!



Biggest Challenges Across the Lifecycle

Several stages of the third-party risk lifecycle present clear challenges due to manual processes.

Finding risk insights is especially difficult during Sourcing.

Calculating exposure is the hardest part of Assessment.

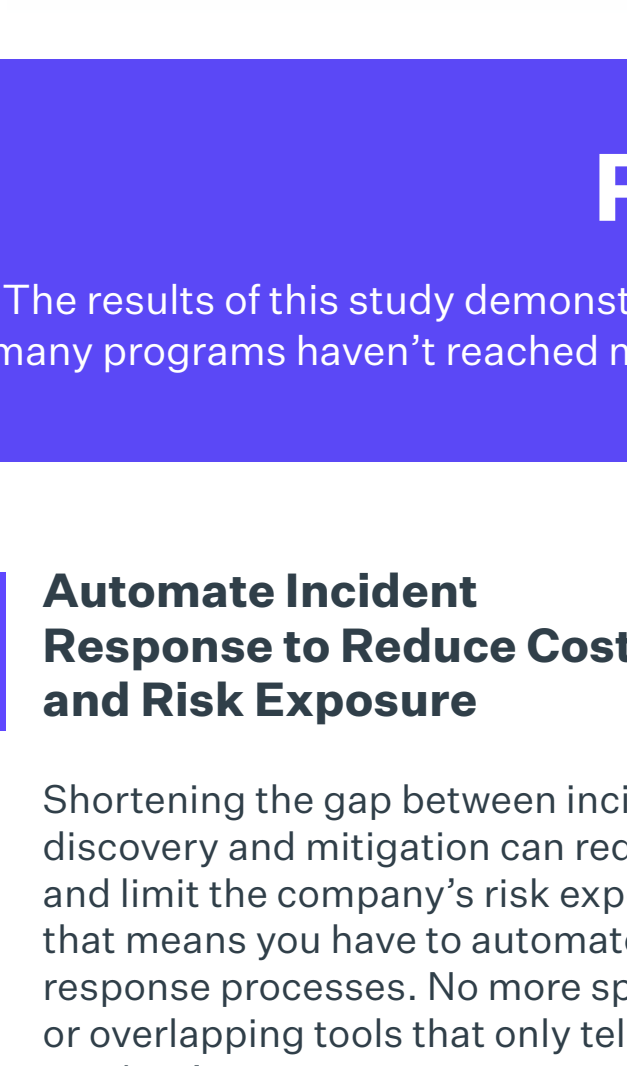
Manual processes are the predominant challenge throughout the TPRM lifecycle.

Perhaps this lack of efficiency is the reason behind the gap between tracking and remediating risks.

Primary Methods of Tracking Risk

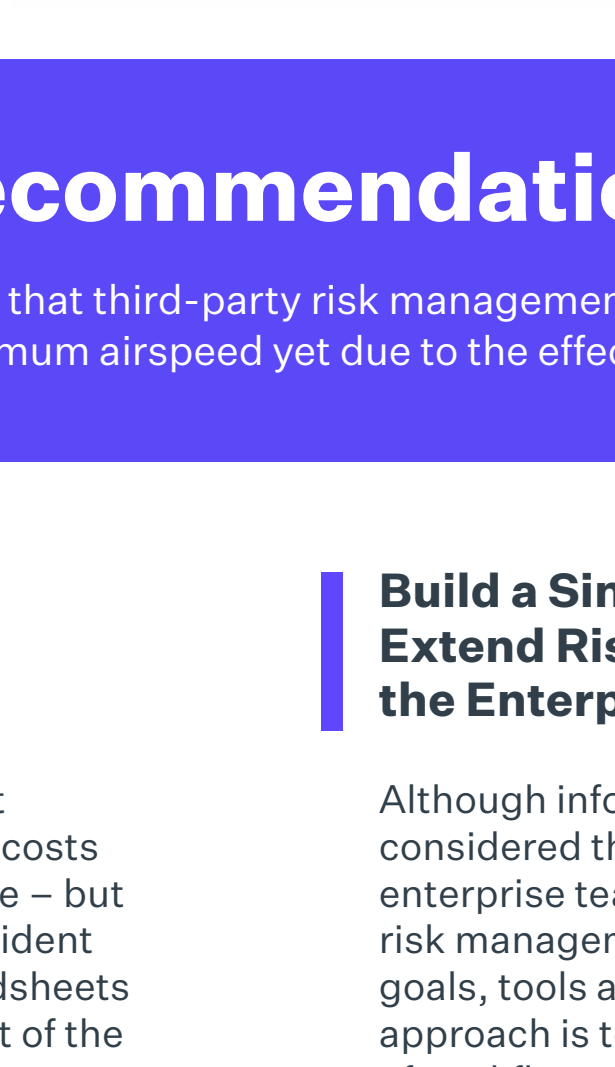
Spreadsheets still represent the #1 method of assessing third-party risk and are mostly used at the Sourcing/Pre-Contract Due Diligence stage (31%).

Risk assessment solutions are popular in the middle stages.



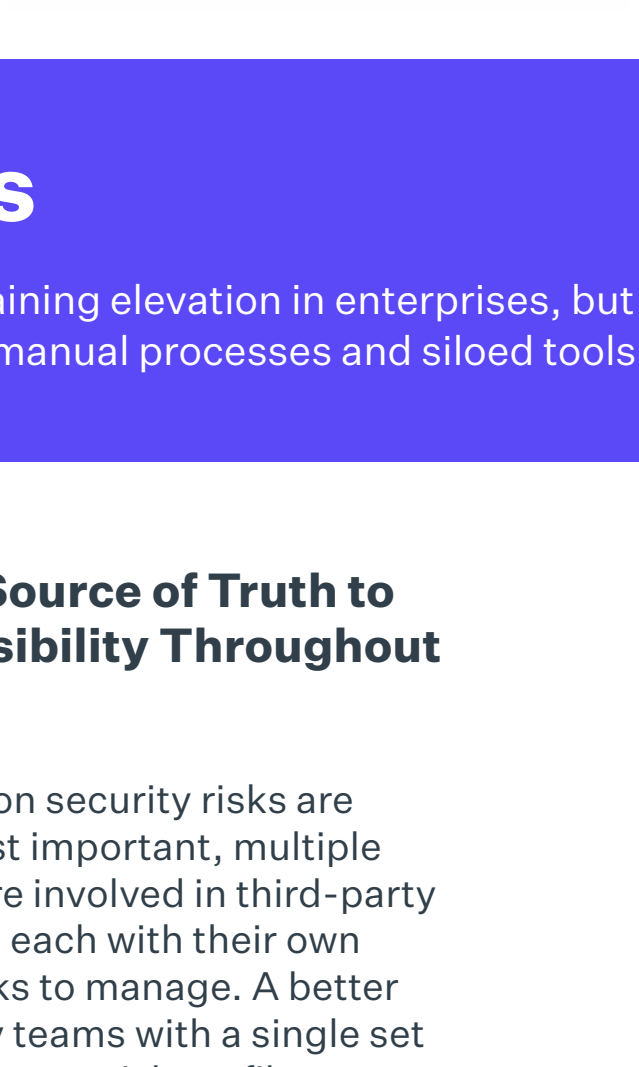
Risk assessment tools were the most popular tool cited by respondents and were reported as the primary tool in 29% of all responses. They are used frequently during the middle stages of the lifecycle.

Spreadsheets are used frequently in the early stages.



Unfortunately, **spreadsheets** followed closely behind, being the cited as the most popular tool used in 24% of all responses – seeing notably heavy usage earlier in the lifecycle.

Risk tracking falls off in the later stages of the lifecycle.



What's worse is **"not tracking risks at this stage"** was the answer in 16% of all responses, with a huge jump during the Offboarding and Termination stage.

Recommendations

The results of this study demonstrate that third-party risk management is gaining elevation in enterprises, but many programs haven't reached maximum airspeed yet due to the effects of manual processes and siloed tools.

Automate Incident Response to Reduce Costs and Risk Exposure

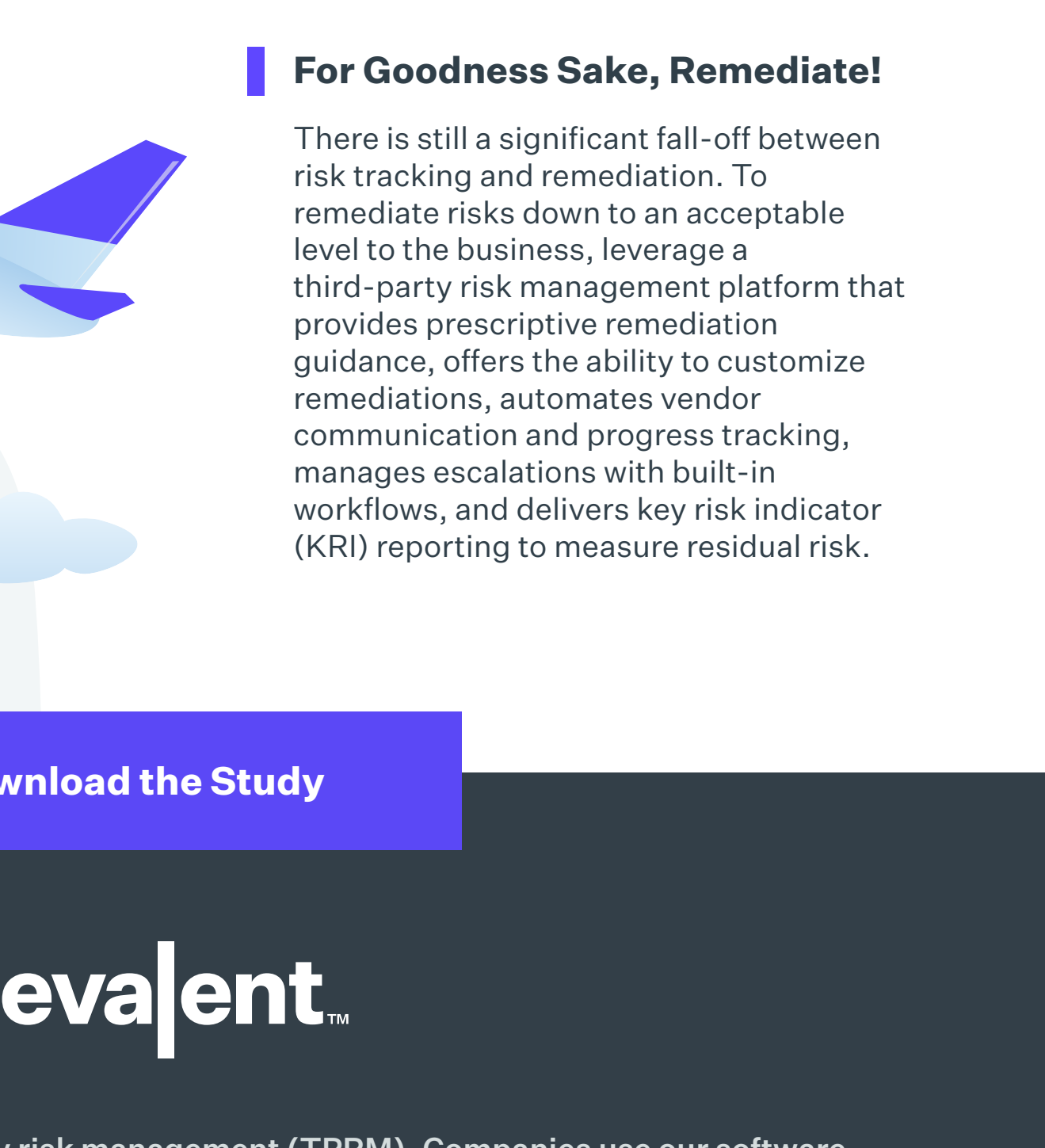
Shortening the gap between incident discovery and mitigation can reduce costs and limit the company's risk exposure – but that means you have to automate incident response processes. No more spreadsheets or overlapping tools that only tell part of the incident's origin story.

Build a Single Source of Truth to Extend Risk Visibility Throughout the Enterprise

Although information security risks are considered the most important, multiple enterprise teams are involved in third-party risk management – each with their own goals, tools and risks to manage. A better approach is to unify teams with a single set of workflows, third-party risk profiles, assessments, and reporting.

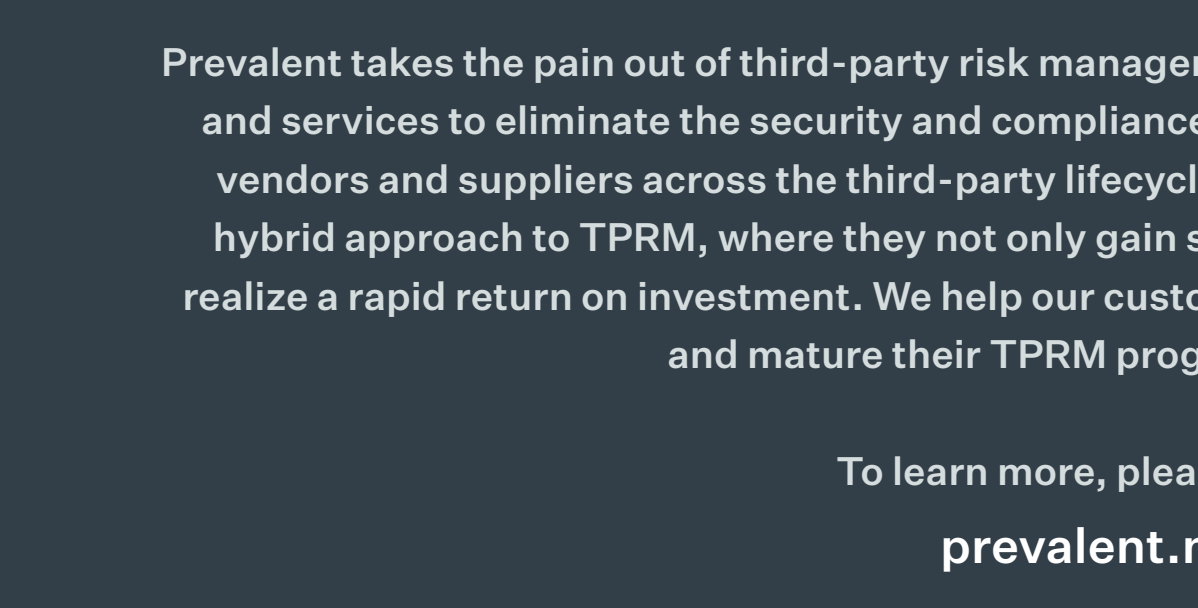
Give Up Spreadsheets and Automate Assessment and Monitoring Across the Lifecycle

Almost of half of organizations are still using spreadsheets to assess third parties. Instead, use a solution that centralizes contract lifecycle management, automates tasks, offers remediation guidance, and delivers a prescriptive process to address final tasks and report according to compliance requirements.



For Goodness Sake, Remediate!

There is still a significant fall-off between risk tracking and remediation. To remediate risks down to an acceptable level to the business, leverage a third-party risk management platform that provides prescriptive remediation guidance, offers the ability to customize remediations, automates vendor communication and progress tracking, manages escalations with built-in workflows, and delivers key risk indicator (KRI) reporting to measure residual risk.



Download the Study

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