Prevalent™

The 2022 Prevalent

Third-Party Risk Management Industry Study

TPRM Programs Are at a Crossroads

Table of Contents

Prevalent™

Introduction

Between February and March 2022, Prevalent conducted a study on 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 third-party risk management programs – specifically as they relate to incident response, compliance, and the vendor lifecycle.

Respondents to the study were directly involved in third-party risk management and worked for enterprises across a variety of industries and sizes.

So, how are organizations navigating today's third-party challenges and staying ahead of future risks? The Prevalent 2022 Third-Party Risk Management Study has the answers.

Summary

What a bumpy road the last year has been. Just when you thought the world had turned the corner from a devastating and chaotic period – BAM! We're witnessing record numbers of third-party data breaches (like Log4j, PracticeMax, Kaseya, and many others), plus supply chain disruptions (like Toyota) from cyber breaches, ongoing pandemic shutdowns in China, and the War in Ukraine.

The good news is that organizations are starting to adapt their third-party risk management (TPRM) programs to address new and emerging risks outside of the IT realm. However, as you will read in this study, third-party risk management is at a crossroads and much more needs to be done. By analyzing these challenges in light of current best practices and modern global realities, we arrived at seven key observations about the state of third-party risk management today:

1. Organizations are paying more attention to non-IT security risks – but not enough.
2. Third-party risk management may (finally!) be getting more strategic.
3. Manual methods for assessing third parties persist but dissatisfaction runs high.
4. Organizations are concerned with increasingly damaging third-party security incidents but are using disparate tools to detect, investigate and resolve exposures.
5. Organizations are waiting over two weeks for third-party incident resolution.
6. Third-party risk audits are getting more complex and time consuming.
7. Third-party risk management discipline falters as vendor relationships progress.

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

Finding #1:

Organizations are paying more attention to non-IT security risks – but not enough.

TPRM programs are still primarily focused on addressing the risks faced when working with IT vendors (45%). It should therefore come as no surprise that the top-weighted risk type that organizations track is information security risk, followed by data privacy and protection – typically the domains of IT security teams.

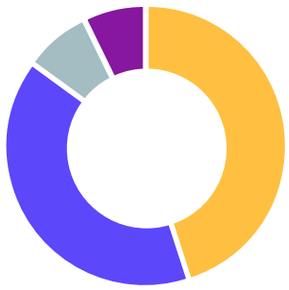
However, a surprising 40% of respondents in this year's survey say they are focused on managing both IT and non-IT vendor risks. This is a positive trend. The appearance of business continuity and reputational and financial risks in the top 5 risk types shows that organizations are acknowledging that third-party risk is about more than IT security risks.

45%

of TPRM Programs Are Mostly Focused on **IT Vendor Risk**

40%

Focused on Both **IT & Non-IT Vendor Risk**



Which statement best describes the focus of your third-party risk management program?

- **45%** - Addressing the risk that we face when working with IT vendors.
- **40%** - Managing the risks associated with all third parties (not just IT vendors).
- **8%** - Tracking events or problems that can impact our supply chain.
- **7%** - Achieving compliance.

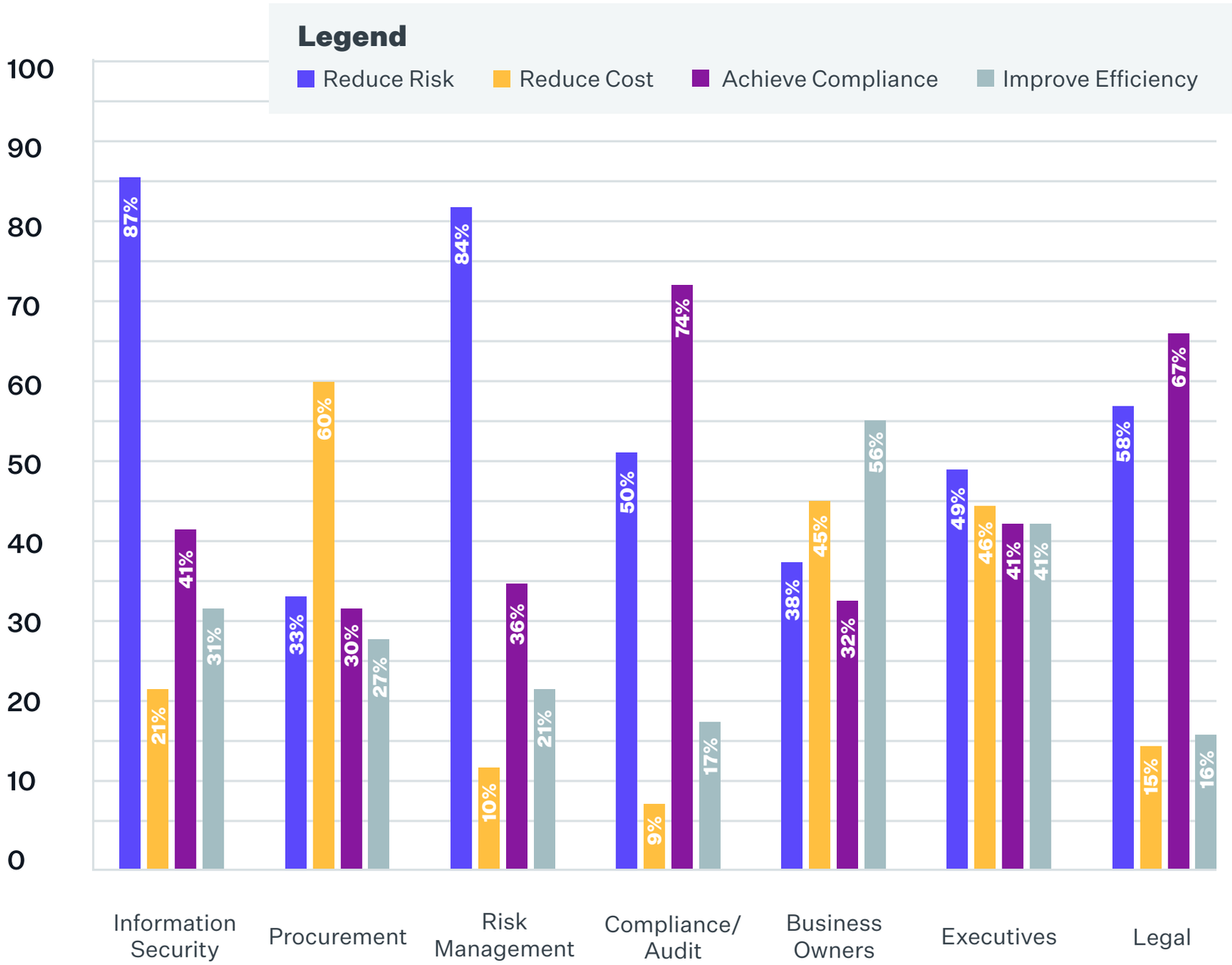
In contrast, risks that respondents weighted the lowest in importance were modern slavery, anti-money laundering, and anti-bribery and corruption risks. Following a similar theme to the Prevalent 2021 Third-Party Risk Management survey, organizations continue to overlook less–quantifiable risks that could still lead to compliance violations, fines, or negative reputational impacts.

Organizations continue to overlook less–quantifiable risks that could still lead to compliance violations, fines, or negative reputational impacts.

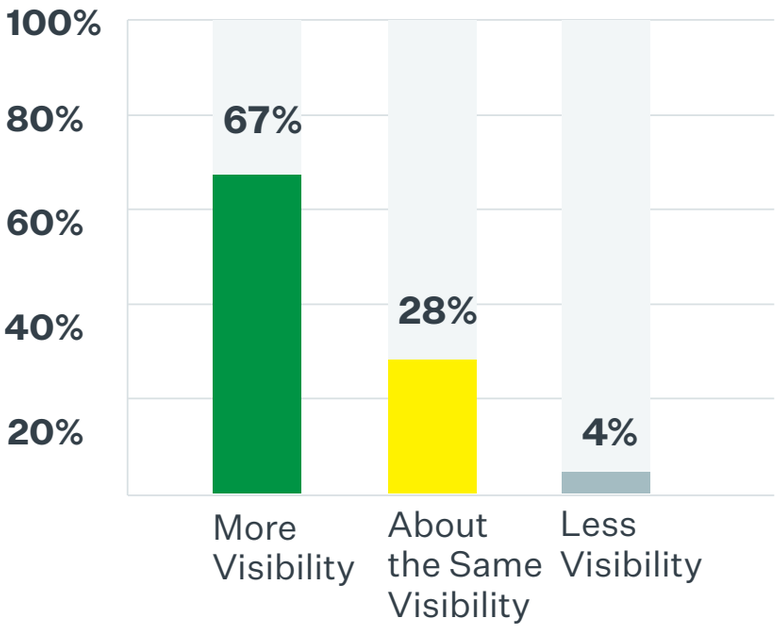
Finding #2:
Third-party risk management may (finally!) be getting more strategic.

Study results show that organizations are generally aligned around the strategic risk reduction goals of their TPRM programs – and that operational concerns such as cost, compliance, and efficiency are secondary. Notably, executives have a fairly even view of TPRM goals across all areas, although they are primarily driven by risk reduction.

What are the goals of your TPRM program?
(by respondent department)



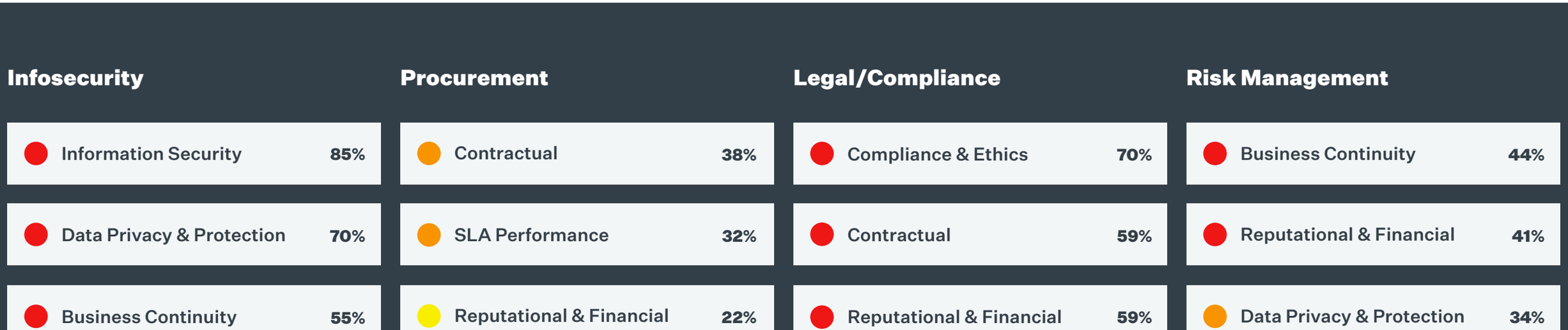
In the last year, has third-party risk management had more or less visibility among executives and the board in your organization?



Speaking of executives, more than ⅔ of respondents indicated that their third-party risk management program has more visibility among executives and the board compared to last year. In our 2021 survey, we learned that 40% of respondents said TPRM had increased visibility among executives, and 36% reported increased visibility among board members.

TPRM is starting to be seen as strategic – likely in response to the massive increases in third-party vendor and supplier-related cybersecurity issues such as Log4j, the Toyota supply chain breakdown, the PracticeMax ransomware attack, and the Kaseya ransomware attack.

Beyond security teams and executives, who else in the organization has an interest in third-party risk management, and what types of risk are they interested in?



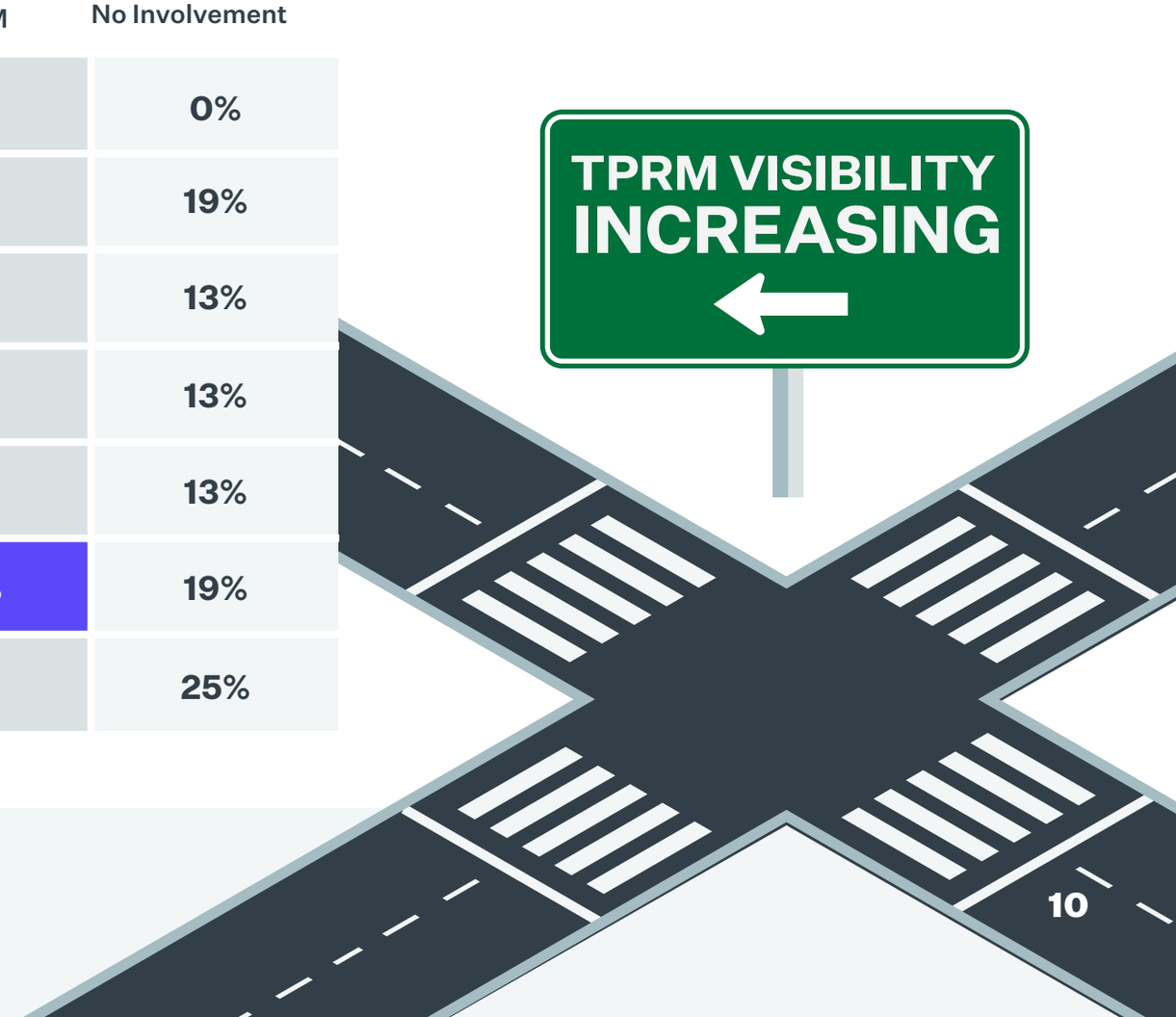
- Procurement teams are most interested in contractual, SLA performance, and reputational and financial risks.
- Legal/Compliance teams are most interested in compliance and ethics, contractual, and reputational and financial risks – somewhat similar to procurement teams.
- Risk management teams are most interested in business continuity, reputational and financial, and data privacy and protection risks.

Who is responsible for third-party risk in your organization?

It should come as no surprise that security and risk management teams are mostly responsible for TPRM program design, strategy, and planning.

Security teams are also responsible for execution of assessments and monitoring. When it comes to using risk information and reports, security takes the lead, but all other departments mentioned here are consumers, too. Finally, it's the executives who are consulted about the program. We're clearly starting to see TPRM visibility improving across the enterprise.

	TPRM Program Strategy, Design and Planning	Execution of Third-Party Assessments and Monitoring	User of Third-Party Information and Reporting	Consulted About TPRM	No Involvement
Information Security	24%	23%	19%	3%	0%
Procurement	12%	16%	16%	19%	19%
Risk Management	24%	13%	16%	5%	13%
Compliance/Audit	10%	14%	16%	14%	13%
Business Owners	9%	14%	16%	16%	13%
Executives	12%	8%	10%	32%	19%
Legal	10%	13%	9%	11%	25%



Finding #3:
Manual methods for assessing third parties persist, but dissatisfaction runs high.

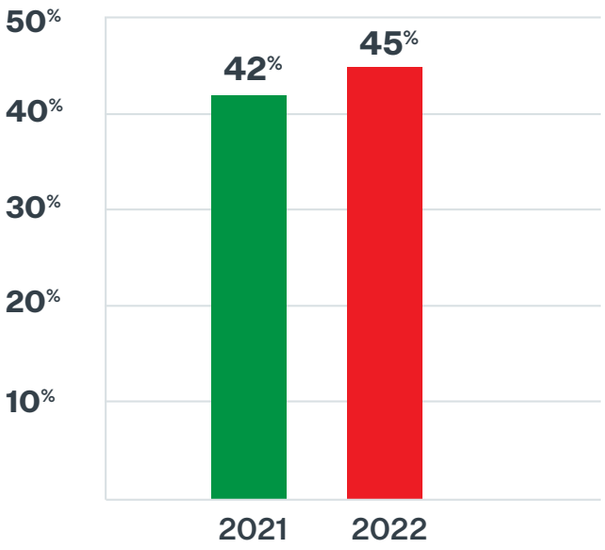
45% of respondents – almost half! – indicate that they are *still* using spreadsheets to assess their third parties. This is a disappointing increase over 2021, when 42% said they were exchanging spreadsheets to assess their third parties.

It's not all doom and gloom, however. Reported use of GRC tools and security rating services is up slightly versus last year. Also, fewer respondents admitted to not assessing their third parties at all. And dedicated TPRM solutions hold the "top-mover" spot in terms of year-over-year increase (14%) among assessment methods. Organizations are finally coming to a realization that they need a comprehensive platform to assess their third parties.

	2021	2022	Change
Dedicated TPRM Solutions	24%	38%	+14%
Spreadsheets	42%	45%	+3%
Security Rating Services	35%	38%	+3%
GRC Tools	21%	22%	+1%
Don't assess third parties	10%	8%	-2%

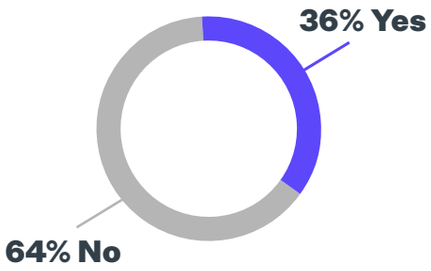
The use of dedicated TPRM solutions grew by 14% from 2021 to 2022, and the use of GRC tools and security rating services rose slightly from last year.

Companies still using spreadsheets to assess their third parties:



Most respondents indicated that their current method of assessing third-party risk can uncover risks across security, business and reputational domains. However, few report having the automation and reporting capabilities they need to demonstrate compliance and satisfy company leadership. In other areas, respondents were split.

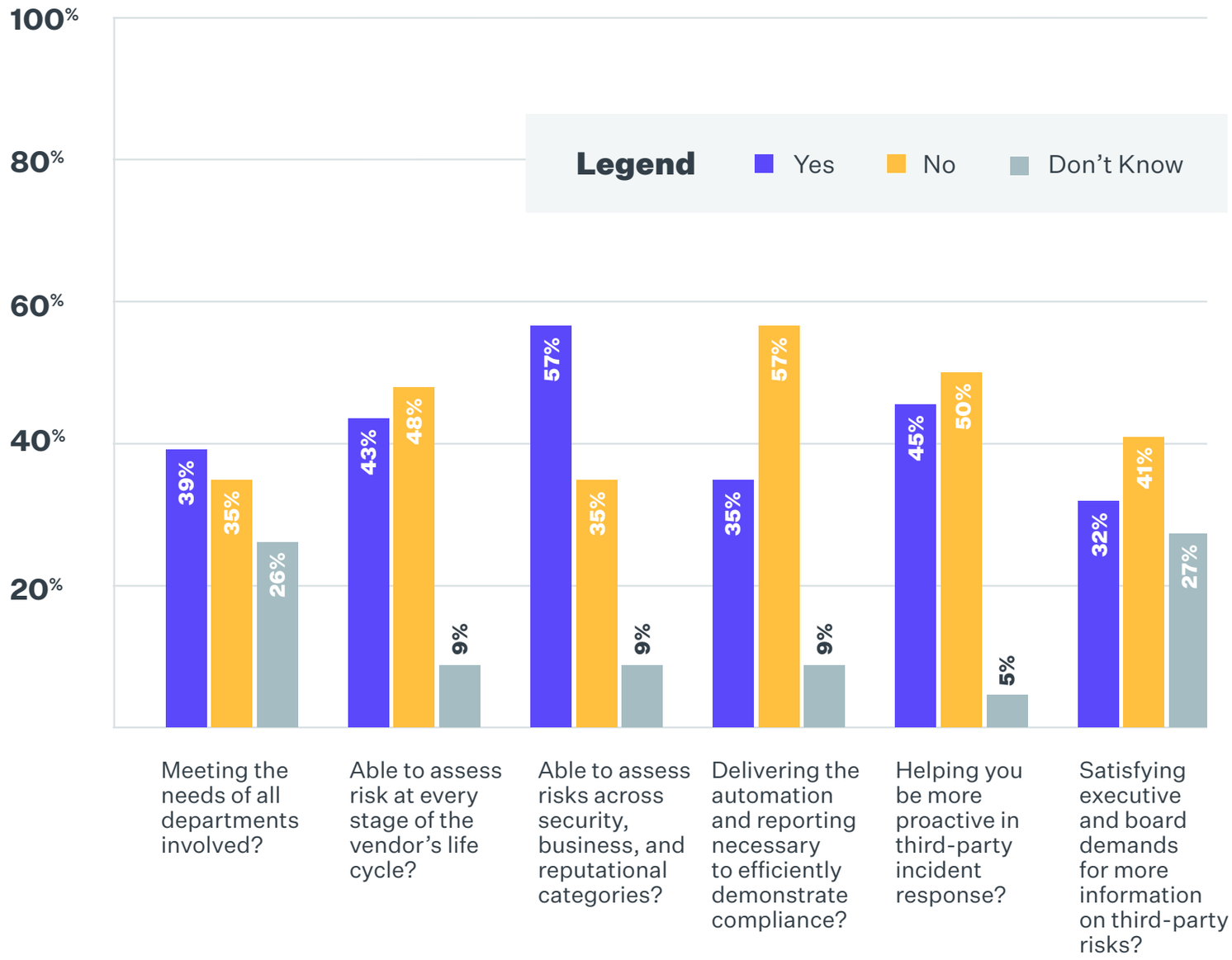
Are you planning to implement a new, or augment/replace an existing, TPRM solution within the next 12 months?



Ultimately, 36% of respondents are planning to either replace their existing solution or implement a new one in the next 12 months.

What does this mean? An organization's chosen method of assessing vendors typically covers the basics: It can assess third parties. But good luck when it comes to reporting and board requests. This is likely a symptom of an overreliance on spreadsheets as the preferred method of conducting third-party risk assessments.

Is your current method of assessing third-party risk:



Finding #4:

Organizations are concerned with increasingly damaging third-party security incidents but are using disparate tools to detect, investigate and resolve them.

The top concern among organizations in the survey is a third-party data breach or other security incident stemming from vendor security shortcomings. In fact, 45% report experiencing a data breach or other security incident connected to a third party in the last 12 months – up dramatically from 2021 when 21% of respondents said their organizations were impacted by a third-party data or privacy breach. **That's more than double!**

What's even more interesting is that 25% of respondents indicated the breach resulted in a significant business impact – from lost customers and reduced revenue, to bad press and steep remediation costs. 55% of respondents said they experienced an auditing finding related to a third party in the last 12 months, up from 10% in 2021. And 54% of respondents said they experienced a supply chain disruption because of a third-party failure, up from 22% last year.

Consider the difference in responses between 2021 and 2022. There was a massive increase in third-party incidents, breaches, compliance issues and supply chain disruptions affecting organizations.

What are the top concerns facing your organization with regard to its usage of third parties?

69%

A data breach or other security incident due to poor vendor security practices

16%

A supply chain disruption due to a supplier/vendor/third-party failure

15%

An audit finding related to a third party.

In the last 12 months has your organization experienced any of the following issues related to your usage of a third party?

	2021	2022
Compliance violation	10%	55%
Supply chain disruption	22%	54%
Security incident	21%	45%

Unsurprisingly, the top incident response tools respondents reported having at their disposal were data breach monitoring (51%), cybersecurity/dark web monitoring (45%), vendor assessments (manual/spreadsheet-based) (43%), and proactive vendor self-reporting (43%).

Only 38% of respondents indicated having access to automated vendor assessments, and just over a fourth of respondents are able to map their Nth-party ecosystems to determine risk in their extended supply chains. 12% said they're not even monitoring for third-party breaches. What's more concerning is that 8% of respondents don't have a third-party incident response program in place at all, while 23% take a passive approach to third-party incident response. Organizations should be aware of the risk of using multiple, non-integrated tools to close the loop on their third-party incident response lifecycle.

If a security incident affected one or more of your third parties today, which of the following response processes or tools are currently at your disposal?

Data breach monitoring	51%	Third- or fourth-party relationship mapping	26%
Cybersecurity/ Dark Web monitoring	45%	News feeds	25%
Vendor assessments: Manual, spreadsheets	43%	We are not monitoring for third-party breaches	12%
Proactive vendor self-reporting	43%	None of the above	3%
Vendor assessments: Automated	38%	Breach monitoring	1%

Which of the following statements is true about your third-party incident response program?

When we learn about security incidents, we reach out to impacted third parties to determine their, and therefore our, exposure.	We learn whether third parties are impacted by a security incident from the third-party notification or a news article and wait for an update.	We have no third-party incident response program in place.
69%	23%	8%

Finding #5:
Organizations are waiting more than two weeks for third-party incident resolution.

29% of respondents indicated that it would take them more than a week to determine which third parties were impacted by an incident, with 35% saying it would take up to two days to determine whether it would result in a disruption in service. 47% of respondents said it would be another week before they knew when the third party had completed its remediation or mitigation steps.

In all, it takes about 2.5 weeks from when an organization learns of an incident to when they receive confirmation of remediation. That's a lifetime for an organization to be vulnerable to a potential exploit.

If one of your suppliers/vendors/third parties has been the victim of a security incident, how long did it take your organization to determine the following?

	Less Than 24 Hours	24 to 48 Hours	48 Hours to One Week	More Than One Week	Unsure
Which third parties were impacted by the incident	10%	19%	19%	**29%**	24%
Whether there would be a disruption in their service or deliverables	15%	**35%**	15%	10%	25%
What remediation of risk mitigation steps the third party was using	10%	25%	15%	25%	25%
When the third party had completed its remediation or mitigation steps	11%	16%	5%	**47%**	21%
When the third party had completed its remediation or mitigation steps	17%	6%	17%	22%	39%

Finding #6:
Third-party risk audits are getting more complex and time consuming.

74% of respondents said that they had to report on third-party data privacy and protection controls, with information security controls coming second at 57%. ESG topics – a relatively new risk area – rank in the middle at 23%, and 18% of respondents indicated they had to report on human trafficking and slavery regulations. Organizations use several standards to benchmark their TPRM programs, with the most common falling under ISO and NIST.

Adding a layer of complexity to an already wide-ranging list of topics for their third-party supply chain or vendor audits, 42% of respondents indicated that they are audited yearly, and 23% are audited on an ad-hoc basis.

When audits happen, 41% of respondents indicate it takes their organization between one week and one month to produce the evidence required to meet regulatory audits. A concerning 32% report taking more than 30 days (and some more than 90 days).

Which of the following types of industry standards or governmental regulations does your organization have to report on?

Data Privacy and Protection	74%	Information Security	57%	None of the Above	11%
Environmental, Social and Governance	23%	Human Trafficking and Slavery	18%		

Which standards does your organization use to benchmark its third-party IT security or privacy practices?

ISO (including 27001, 27002, 27018, 27036-2, 27701 or others)	54%	NIST (including 800-53, 800-61, 800-161, Cybersecurity Framework or others)	49%	We do not assess our third parties against industry or government standards	12%
SOC 2	38%	Standard Information Gathering (SIG)	25%		

How frequently is your organization audited for third-party risk management practices?

Yearly	42%	Quarterly	21%	We are not audited	9%
Ad-hoc	23%	Whenever there is an incident	4%		

How long does it take your organization to produce the reporting and evidence required to meet regulatory audits?

Less than 1 week	27%	Between 1 week and 1 month	41%
Between 30 and 90 days	23%	More than 90 days	9%

Finding #7:
Third-party risk management discipline falters as vendor relationships progress.

About ¾ of respondents are tracking risks at the sourcing/pre-contract due diligence and onboarding stages of the third-party relationship, which is good but not great. That leaves about a fourth of companies that don't conduct risk assessments at this crucial stage, meaning they're exposed to potential risks from the start of the relationship.

Between 61% and 68% of respondents are tracking risks at the "business as usual" phases – assessing, monitoring and ongoing management. Still a somewhat low number.

What's most surprising is that fewer than half of respondents are tracking contractual risks and risks at the offboarding and termination stage of the relationship.

In fact, the percentage of customers tracking risks declines as the relationship lifecycle matures, indicating that companies are focused more on risks at the earliest stages, less so as the relationship continues. Yet, we see that risks are present throughout the vendor lifecycle.

	Currently Tracking Risks	Not Currently Tracking Risks	Don't Know
Sourcing & Pre-Contract Due Diligence	74%	22%	4%
Onboarding	78%	17%	4%
Assessing & Monitoring	68%	27%	5%
Ongoing Management	61%	35%	4%
Contractual Performance	45%	41%	14%
Offboarding & Termination	43%	43%	13%

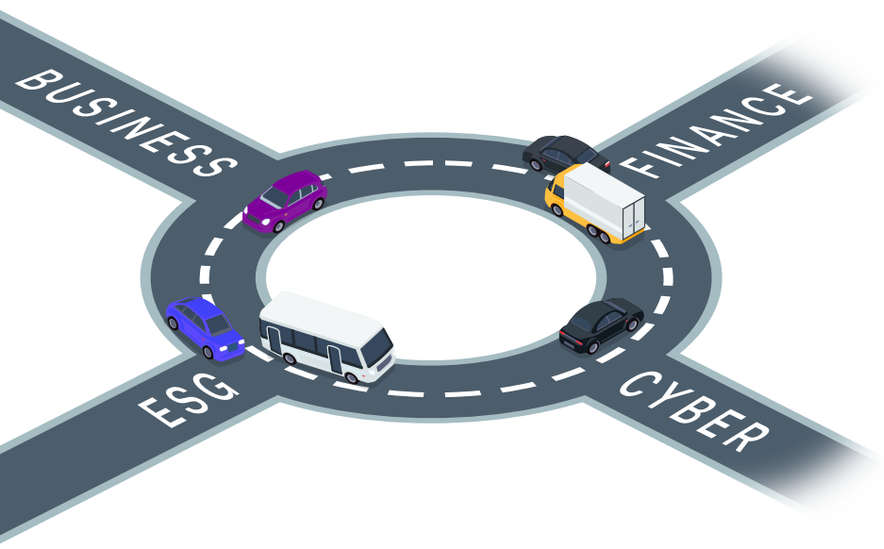
Recommendations

The results of this study demonstrate that third-party risk management teams are making progress toward a more strategic approach to TPRM, but three areas require additional improvements.

Recommendations

Expand Assessments Beyond IT Security to Unify Teams Under a Single Solution and Simplify Audits

Results of the study show that different departments have different TPRM requirements, so looking at third-party risk solely through an IT lens will miss important risks. As evidenced by the developing fallout from the Russian invasion of Ukraine, you can't ignore risks like geopolitical unrest, bribery, corruption and sanctions.



Therefore, invest in a solution that includes built-in questionnaire templates and intelligence to address areas including:

- Business/operational risks such as business resilience, performance and contractual adherence
- Financial risks such as credit problems, bankruptcies and other financial issues
- ESG risks such as environmental violations, health and safety problems, labor and modern slavery concerns, and diversity and ethics issues
- Reputational risks such as sanctions, involvement with state-owned enterprises, and adverse media coverage
- Compliance risks such as regulatory findings, bribery, corruption and money laundering

By unifying non-IT risk intelligence with the results of traditional cybersecurity and data privacy assessments, you can enrich visibility into supplier risks while meeting the needs of multiple departments. This, in turn, elevates the strategic value of your third-party risk management program. It also improves reporting and eliminates the persistent use of spreadsheets to collect and analyze third-party risk data.

In addition, considering that nearly a third of companies say it takes more than 30 days (and some more than 90 days) to produce the evidence required to meet regulatory audits, collecting these insights in a single platform will accelerate audit reviews and enable to teams to get back to their day jobs.

Recommendations

Automate Incident Response to Reduce Cost and Time

The significant year-over-year increase in the number of companies that experienced a third-party security incident is concerning enough. But when you factor in the fact that 25% experienced a significant business impact, it should be no surprise considering that it takes more than two weeks to resolve an incident due to using multiple, non-integrated tools (and in some cases spreadsheets!).

How do you automate incident response? Invest in mature tools and processes that:

- Centrally manage all vendors in a single platform – gaining visibility into your third-party ecosystem is the first and most important step
- Know which third parties (and Nth parties) are at risk from a breach by mapping supplier relationships based on technology usage
- Ask the right questions of the right vendors with contextual event assessment questionnaires
- Get early warning of incidents by enabling vendors to proactively submit event assessments
- Reveal potential impacts by continuously tracking, scoring and managing cyber, business, reputational, and financial risks in a single platform
- Quickly mitigate risks to your business with access to prescriptive remediation guidance
- Satisfy the needs of regulators, board members, and other stakeholders with proactive reports on incident response progress and mitigations

Recommendations

Close the Loop on the Third-Party Lifecycle

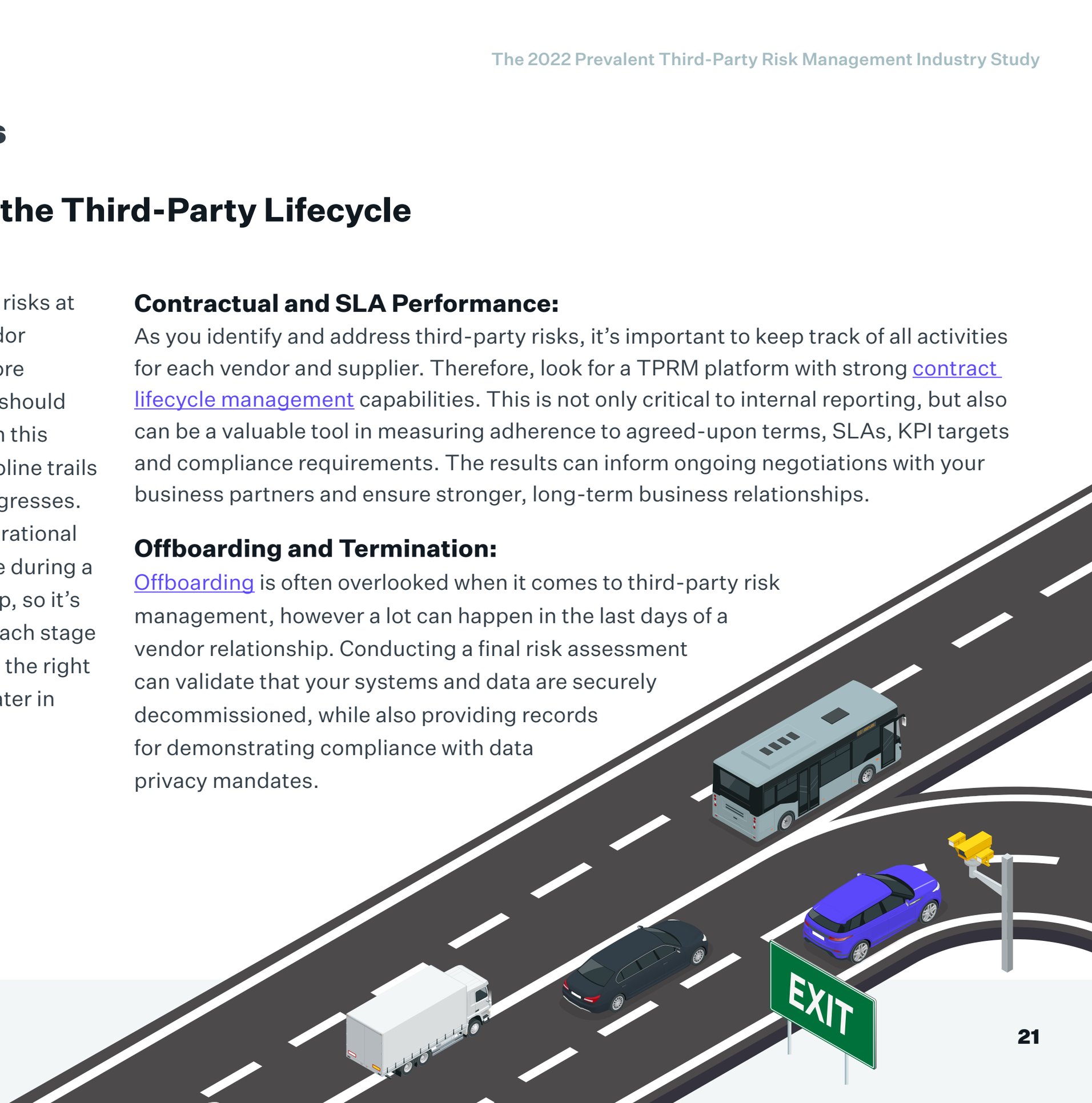
Tracking vendor and supplier risks at the earliest stages of the vendor relationship (for example before contracting and onboarding) should be a no-brainer. But data from this year's study shows that discipline trails off as the vendor lifecycle progresses. Security, compliance and operational issues can crop up at any time during a vendor or supplier relationship, so it's important to address risk at each stage of the third-party lifecycle. To the right are tips for addressing risks later in the relationship.

Contractual and SLA Performance:

As you identify and address third-party risks, it's important to keep track of all activities for each vendor and supplier. Therefore, look for a TPRM platform with strong contract lifecycle management capabilities. This is not only critical to internal reporting, but also can be a valuable tool in measuring adherence to agreed-upon terms, SLAs, KPI targets and compliance requirements. The results can inform ongoing negotiations with your business partners and ensure stronger, long-term business relationships.

Offboarding and Termination:

Offboarding is often overlooked when it comes to third-party risk management, however a lot can happen in the last days of a vendor relationship. Conducting a final risk assessment can validate that your systems and data are securely decommissioned, while also providing records for demonstrating compliance with data privacy mandates.



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, suppliers and other third parties across the entire vendor 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.

Ready to get started?
Request a demonstration to schedule a discussion with a solution expert today.

Prevalent™