Prevalent™

The 2021 Prevalent

Third-Party Risk Management Study

Looking Beneath the Cyber Risk Surface

Table of Contents

Introduction

In February and March 2021, Prevalent conducted a study on current trends, challenges and initiatives impacting third-party risk management practitioners worldwide.

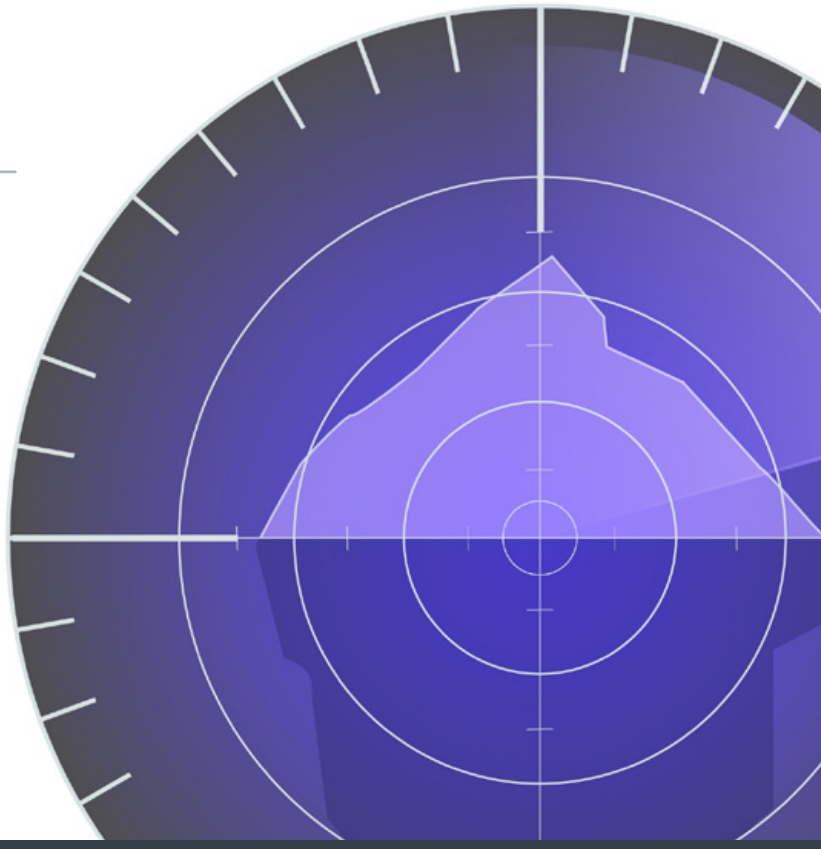
The goal of the study was to provide a state-of-the-market on third-party risk with actionable recommendations that organizations can take to grow and mature their programs across every stage of the third-party risk lifecycle.

Respondents to the study were:

- **Practitioners:** All survey respondents were involved in third-party risk management.
- **Primarily Working in IT and Security:** 76% of respondents work in either IT or IT security at their organizations.
- **Representing Mid-Sized to Enterprise Organizations with Large Vendor Ecosystems:** 76% of respondents work for companies with more than 1,000 employees, with an average of almost 2,400 third parties, and the majority of respondents say up to 30% of their third parties are considered top tier.
- **From a Diverse Set of Industries:** The top 5 respondent industries included:
  - Healthcare/Pharmaceuticals
  - Education
  - Financial Services/Banking
  - Software & Technology
  - Manufacturing/Construction

How are organizations addressing today's third-party challenges and making sure that future risks are on their radar?

The Prevalent 2021 Third-Party Risk Management Study has the answers.



Summary

All organizations rely on vendors and suppliers to power their operations, but working with third parties also means incurring risk. Over the past year, we witnessed mounting scrutiny and penalties tied to regulatory and data privacy requirements; significant third-party breaches that led to customer losses and legal actions; countless supply-chain disruptions associated with the COVID-19 pandemic; and evolving corporate ethics policies spurred by pushes for racial and social justice. While each of these factors spotlights the importance of managing third-party risk, gaining an understanding of vendor controls and policies can be an elusive target to hit.

The reality is, you start taking on risk before you even onboard a vendor, and the results of our 2021 TPRM study reveal that most organizations are struggling to catch up. Challenges cited by respondents include a lack of pre-contract due diligence into vendor controls and policies; the inability to predict potential issues due to outdated and incomplete vendor risk information; and a focus on cybersecurity issues that overshadows equally important factors such as ESG, company reputation, and SLA performance.

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

1. Organizations Are Missing Important Risks – at Their Own Peril

Consider two of the biggest events of 2020: COVID-19 and the social and racial justice movements. Both events fall outside cybersecurity, which is TPRM's traditional "comfort zone." However, the pandemic meant supply-chain and vendor performance problems for many risk management practitioners, with 83% of study respondents reporting increased organizational focus on third-party risk as a result. At the same time, the ongoing justice movements are underscoring the importance of working with partners who have sound diversity and ESG policies. Despite this, we found that few companies are actively tracking third-party risks related to labor standards, the environment and human rights.

2. Attention Should Be Paid to More Stages in the Third-Party Risk Lifecycle

The number-one challenge cited by study respondents was a lack of pre-contract due diligence, which is when risks are assessed prior to contracting with or onboarding a vendor. And, although most organizations claim to assess risks at the early sourcing and selection stage of the vendor lifecycle, the same can't be said for the offboarding stage at the end of the relationship. In fact, 59% of companies say they are not actively assessing third-party risks during offboarding. What's more, almost half of respondents reported having a lack of real-time insights into vendor risk and performance. This is concerning, since failing to cover the gaps between periodic vendor assessments leaves organizations exposed to a constantly evolving threat environment.

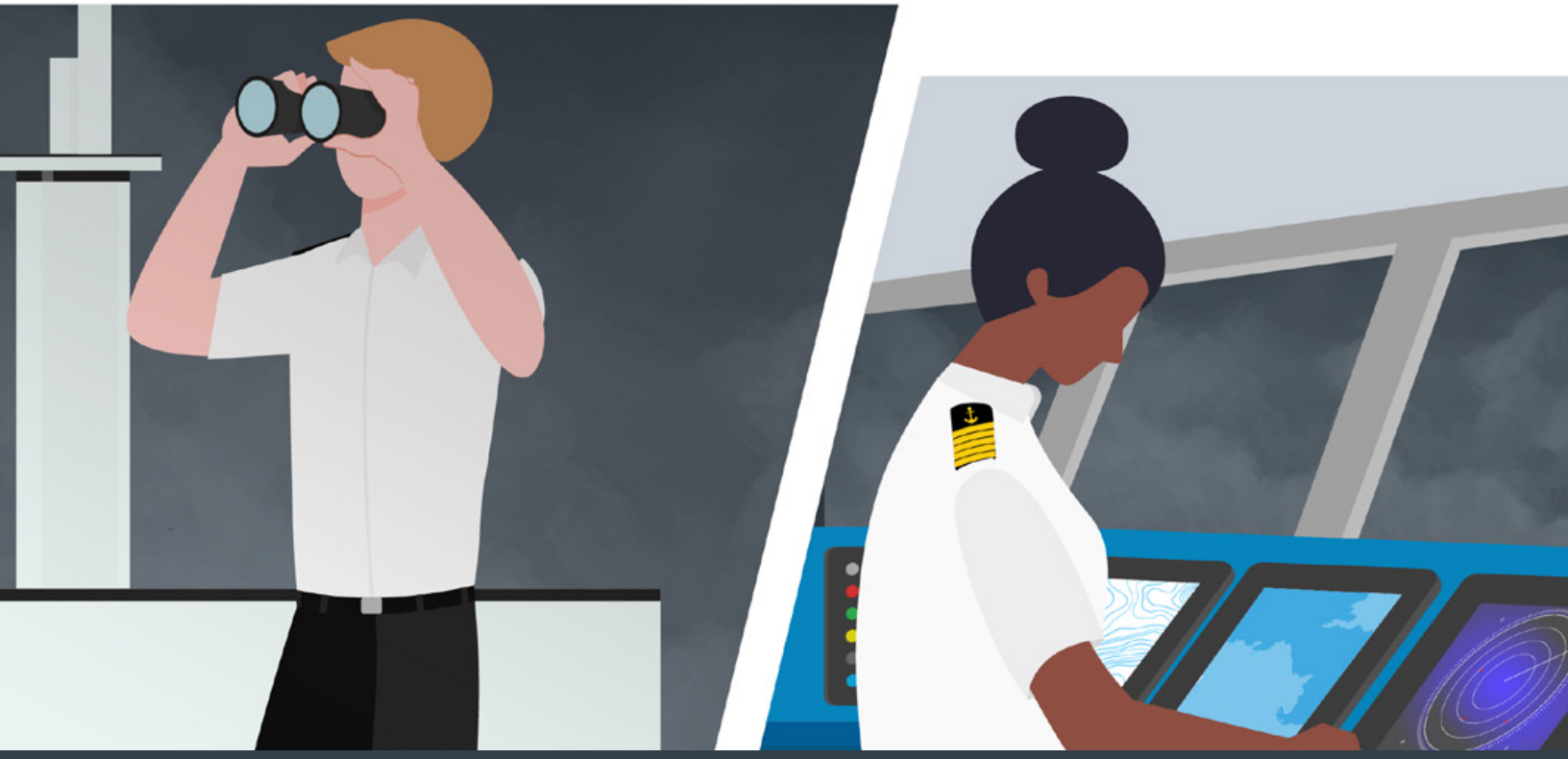
3. Procurement and Business Teams Are Struggling for a Seat at the TPRM Table

50% of respondents report that IT and security own TPRM in their organizations, which is no surprise given the recent spate of headline-grabbing third-party data breaches. The other 50% report ownership by procurement, legal and compliance, vendor management, risk management, and other non-technical teams. However, the data shows that the pendulum is swinging strongly in IT and security's favor in terms of both ownership and involvement in TPRM. For instance, 55% of organizations have seen an increase in ownership by security over the past year, while only 22% have seen an increase in ownership by procurement. This shift is a cause for concern considering the preponderance of third-party threats falling outside the realm of cybersecurity (see observations #1 and #2).

4. Most Organizations Don't Want to Tackle Third-Party Risk on Their Own

When asked about the ideal way to solve their third-party risk challenges, respondents indicated a preference for a hybrid approach that enables them to manage some assessments themselves and outsource the rest. What's more, 70% of respondents indicated that some form of outsourcing is preferred. Why? Because a significant number of practitioners (42%) are still stuck with spreadsheets as the primary mechanism for performing third-party risk assessments – and 65% aren't exactly thrilled about this approach, giving a dissatisfied (26%) or neutral (39%) rating. It's no wonder that respondents report relatively low confidence in their ability to scale their TPRM programs, while citing the importance of a broad range of vendor risk intelligence sources as key to program success.

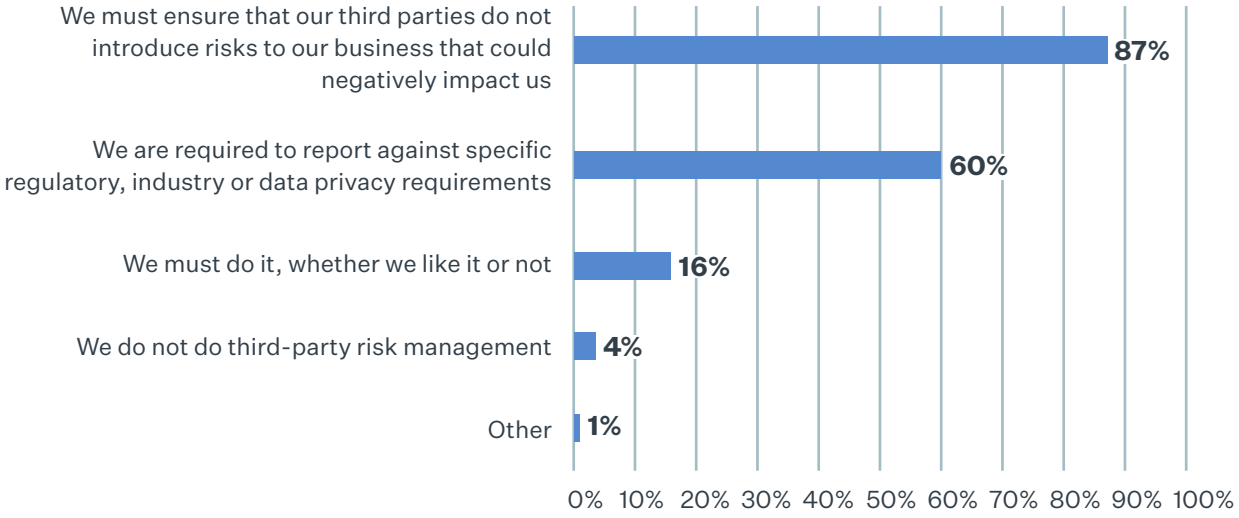
In the following pages, we'll share the detailed response data with further analysis from our experts. We'll also provide recommendations for bridging the gap between IT security and business for more complete and efficient risk management throughout the vendor lifecycle.



Finding #1: When It Comes to Third-Party Risk, Cybersecurity Is the Tip of the Iceberg

Let's begin by looking at why organizations assess third parties. The vast majority of respondents (87%) cited the need to ensure that third parties do not introduce risks to their business that could negatively impact them, followed by 60% who say that they are required to report against specific regulatory, industry or data privacy requirements. This represents a shift from when compliance was the primary driver for TPRM programs.

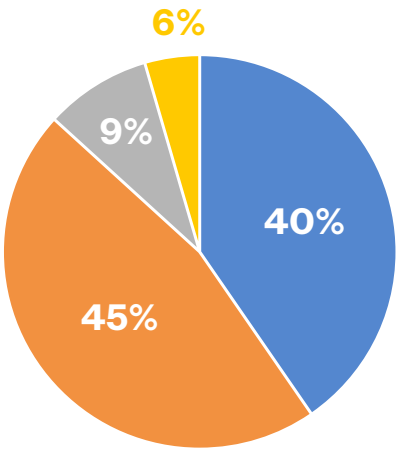
Why do you assess third parties?



But are TPRM programs keeping up? Respondents to the survey are roughly split between whether their program is expanding (40%) or in a steady state (45%).

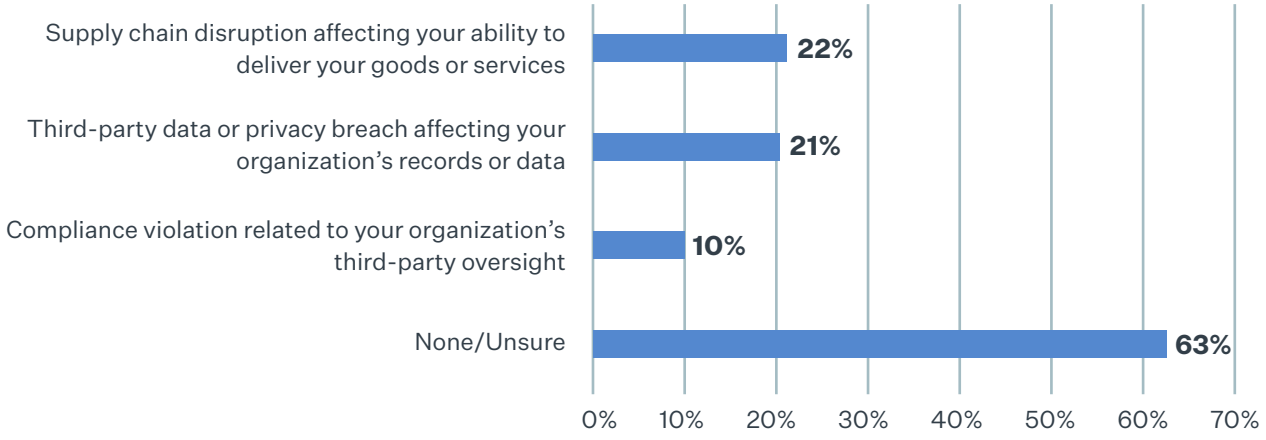
Which statement best describes your TPRM program?

- Expanding: **40%**
- Steady State: **45%**
- Reducing: **9%**
- Nothing in Place: **6%**



It is somewhat surprising to see a relatively lower number as "expanding" (40%) considering that more than **50% of organizations have been impacted by supply-chain disruptions, third-party data breaches or compliance violations in the past year.**

How has your organization been impacted by any of the following in the past year?

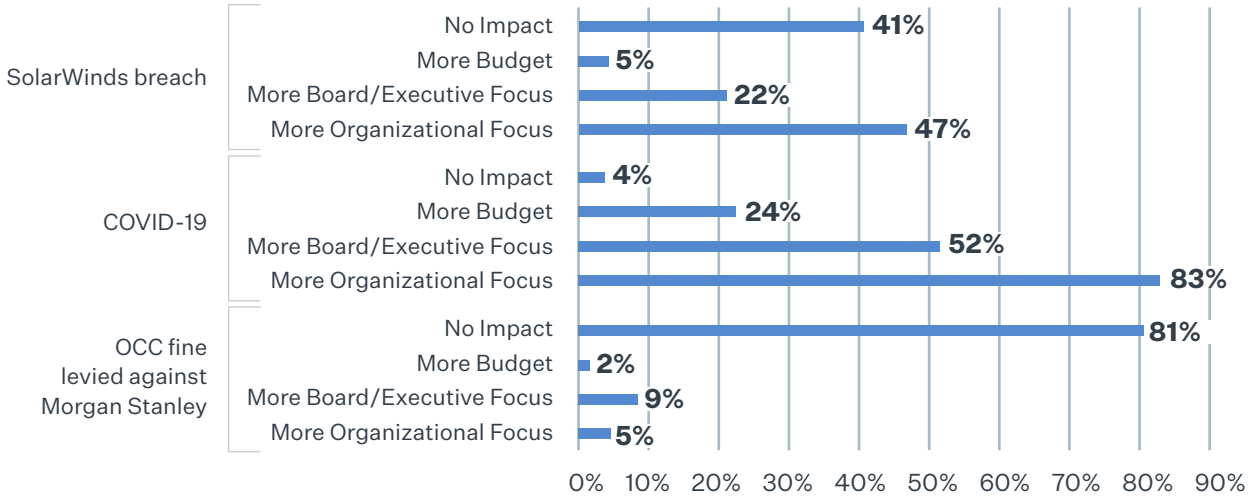


The consequences of events like these over the last two years have been significant – especially in terms of lost productivity (27%) and monetary damages (17%).

What negative impacts has your organization experienced in the last two years?

Consider three of the most significant third-party risk management developments in the last 12 months: the SolarWinds breach, COVID-19, and the $60 million OCC fine of Morgan Stanley. **COVID-19 (83%) and the SolarWinds breach drove the most organizational focus on third-party risk**, and more board/executive focus.

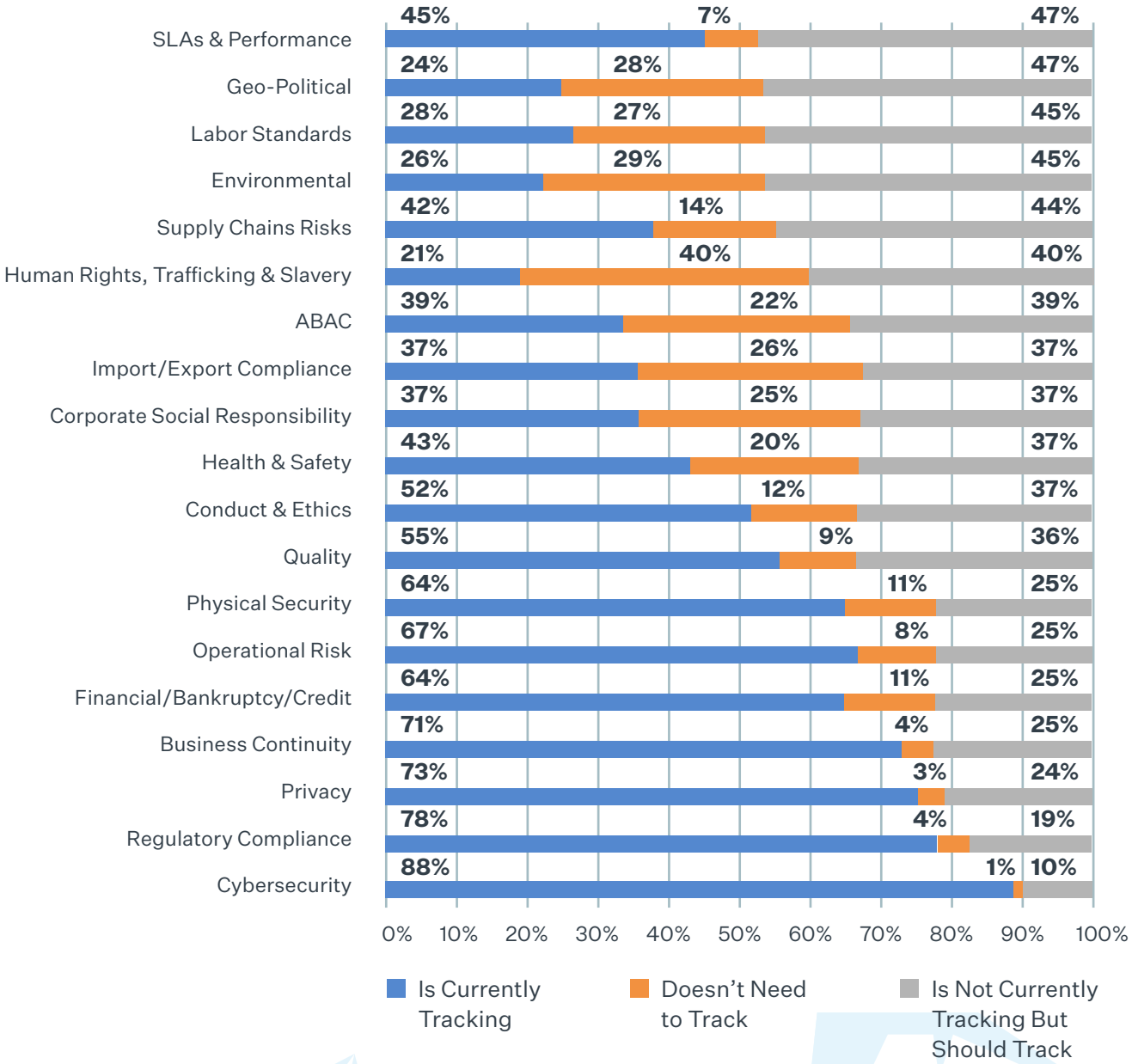
How have the following developments impacted your company in the last year?



It's no surprise that the top risks tracked by organizations today include **cybersecurity (88%)**, regulatory compliance, privacy and business continuity. These are core assessment targets for IT security teams, who are also the primary owners and influencers over TPRM programs (as we'll see later in the report).

On the other hand, risks that organizations report not tracking, but should be, include **SLAs and performance (47%), geo-political (47%), labor standards (45%), environmental (45%), supply chain (44%), human rights, trafficking and slavery risks (40%), and ABAC (39%)** – perhaps a consequence of the relative lack of involvement by procurement and other business teams. It's clear that organizations must expand the scope of their assessments or risk missing important indicators that could impact their third parties' abilities to deliver in today's business environment.

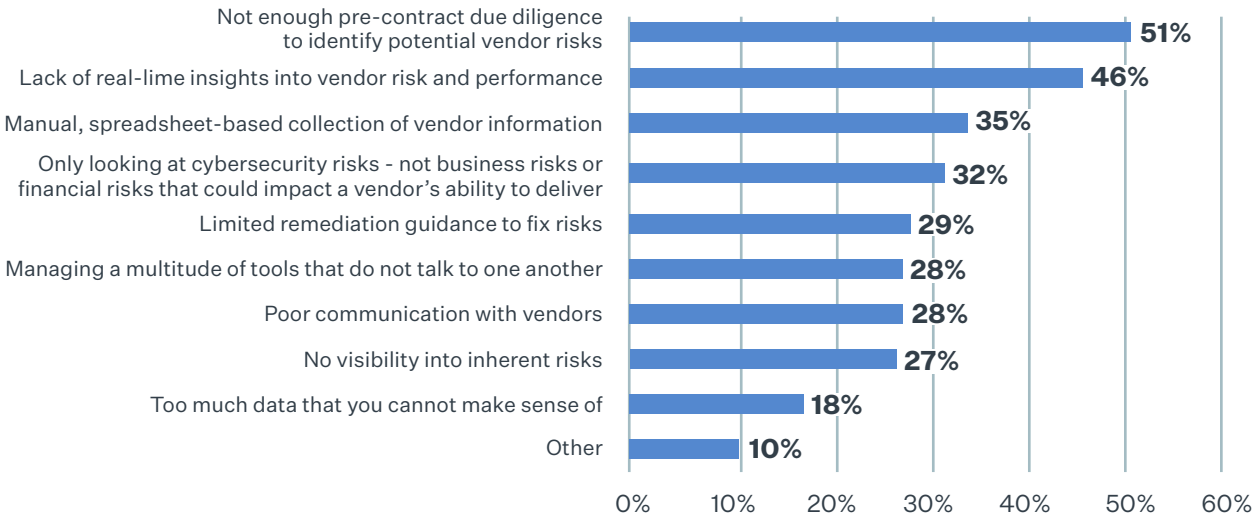
Types of risks that your organization...



Finding #2: Organizations Are Missing Risks at Critical Stages of the Vendor Lifecycle

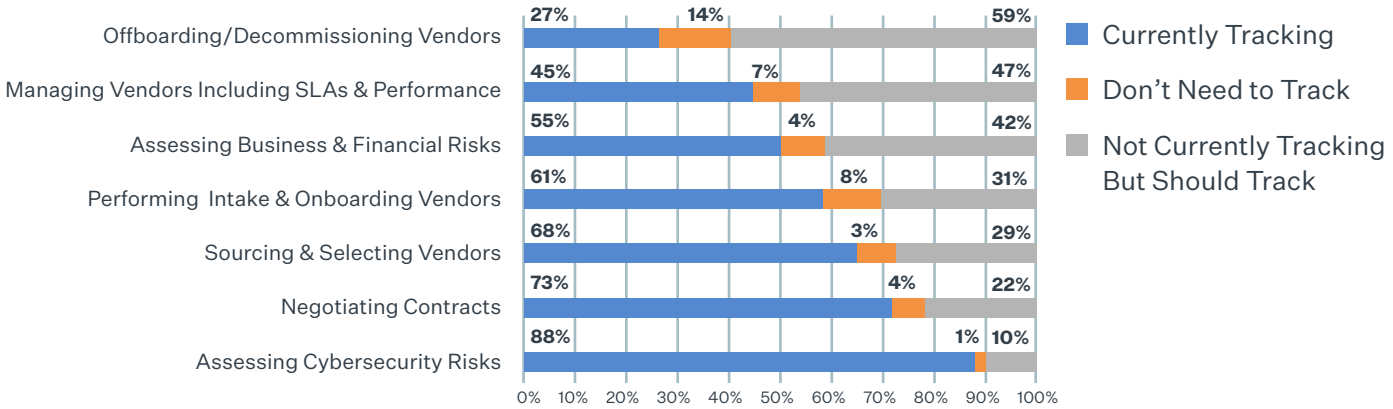
More than 50% of respondents indicated the biggest challenge they face in third-party risk management is not having enough pre-contract due diligence to identify potential vendor risks, followed by 46% who say a lack of real-time insights into vendor risk and performance is their biggest challenge. This is an understandable challenge considering that most respondents have not yet extended their risk assessments beyond traditional cybersecurity topics.

What are the biggest challenges you face in third-party risk management?



We also asked about when organizations assess risk during the vendor lifecycle. Respondents most frequently report assessing cybersecurity risks (naturally), while negotiating contracts, and while sourcing and selecting vendors. However, with such little involvement in third-party risk management, are procurement and business teams getting the visibility they need at the sourcing and selection and contract negotiation stages? Read on to find out. How about offboarding and decommissioning? **59% of respondents are not tracking risks** at this stage but feel they should.

Tracking risks by stage of the third-party lifecycle

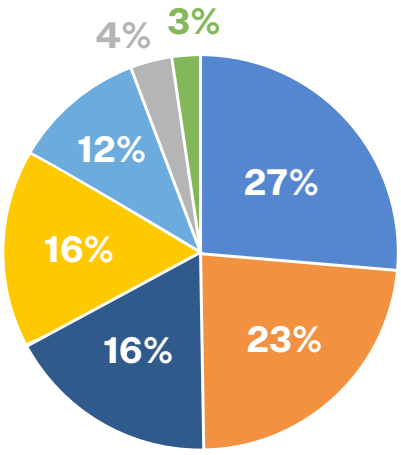


Finding #3: Third-Party Risk Management Needs Broader Ownership and Stakeholder Influence

50% of survey respondents indicated that IT or IT security owns third-party risk management in their organizations, with smaller numbers saying that legal/compliance, risk management or procurement owns it.

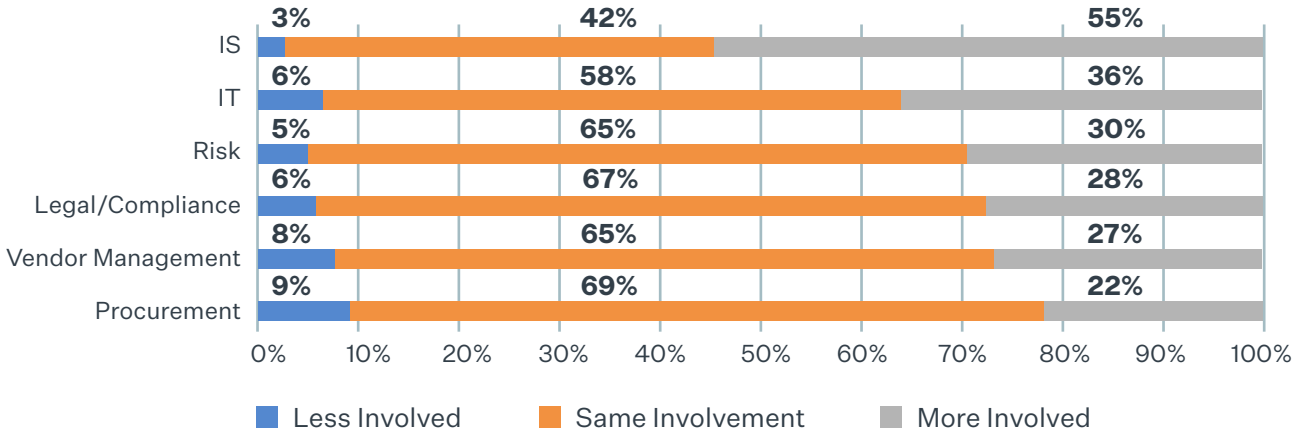
Who owns third-party risk in your organization?

- IT: **27%**
- Information Security: **23%**
- Legal/Compliance: **16%**
- Risk Management: **16%**
- Procurement/Purchasing: **12%**
- Other: **4%**
- Vendor Management: **3%**



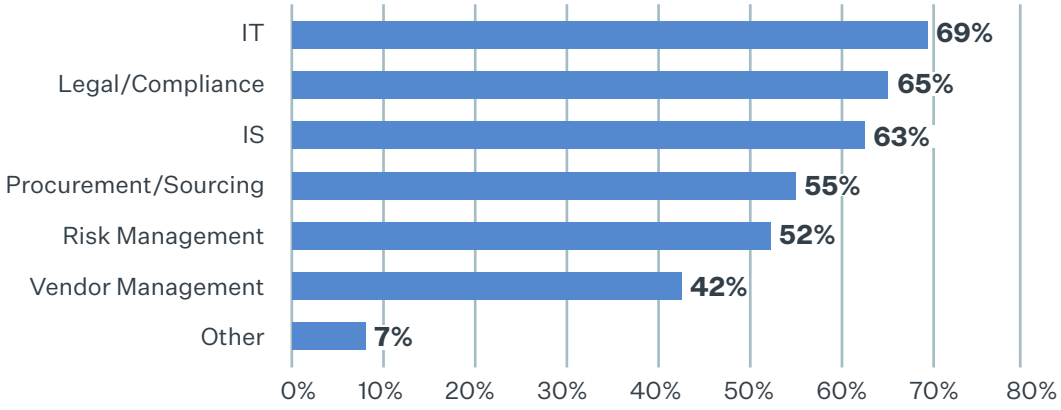
Perhaps unsurprisingly given the recent spread of third-party data breaches, **more than half of organizations (55%) say that IT security teams were even more responsible for third-party risk management in the last year.** This increased responsibility appears to have come at a cost, though: Procurement teams are seeing the least growth in TPRM responsibility at 22%, and the most decline in responsibility at 9%. The question remains whether the needs of procurement and other business teams are sufficiently being met.

How has this responsibility changed in the last 12 months?



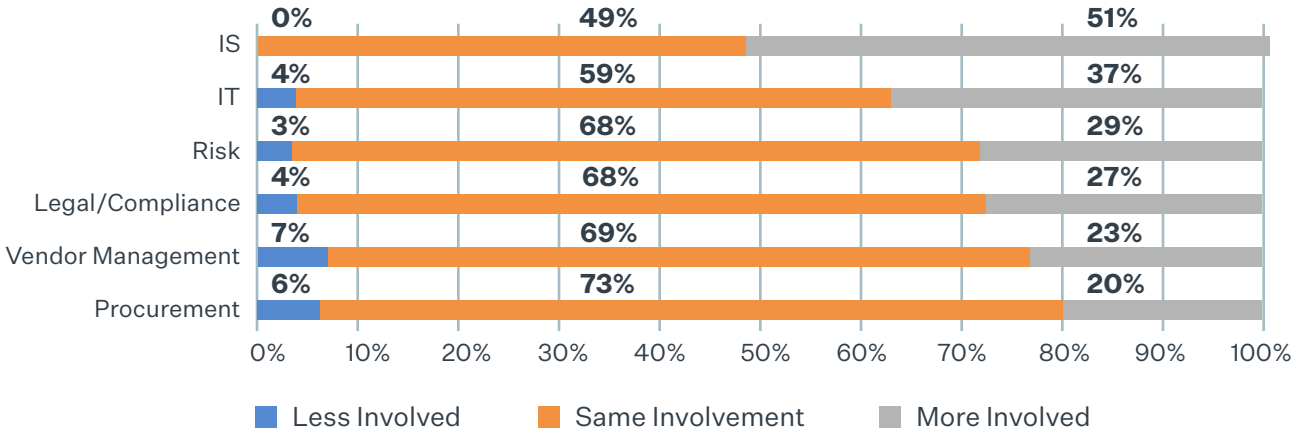
Many departments have a stake in third-party risk management, with IT, legal/compliance, IT security, procurement and risk management making up the top 5.

Which departments have a stake in TPRM?



As with ownership over third-party risk management, IT security teams have increased their stake – or involvement – the most in the past 12 months, with procurement teams again having the least amount of growth in involvement.

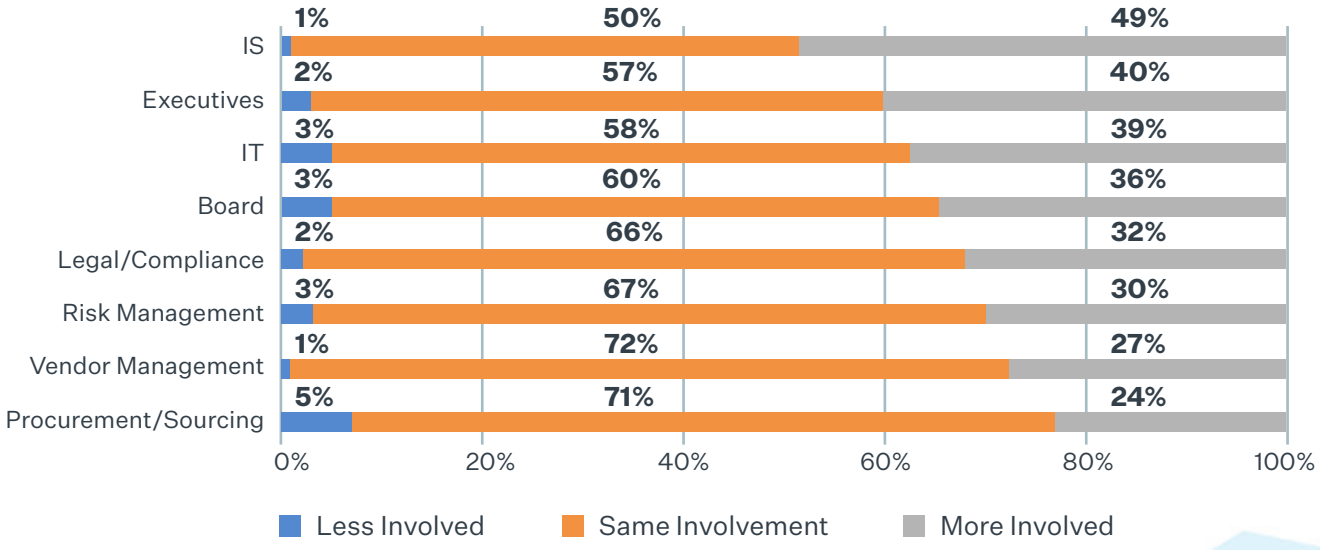
How have these departments' stakes in TPRM changed in the last 12 months?



Third-party risk management is gaining increased visibility in enterprises, primarily among IT security teams, executives (40%) and boards of directors (36%) – likely in response to aforementioned breaches. The question IT security teams need to answer is this:

Will board visibility trigger a call for expanded risk assessments?

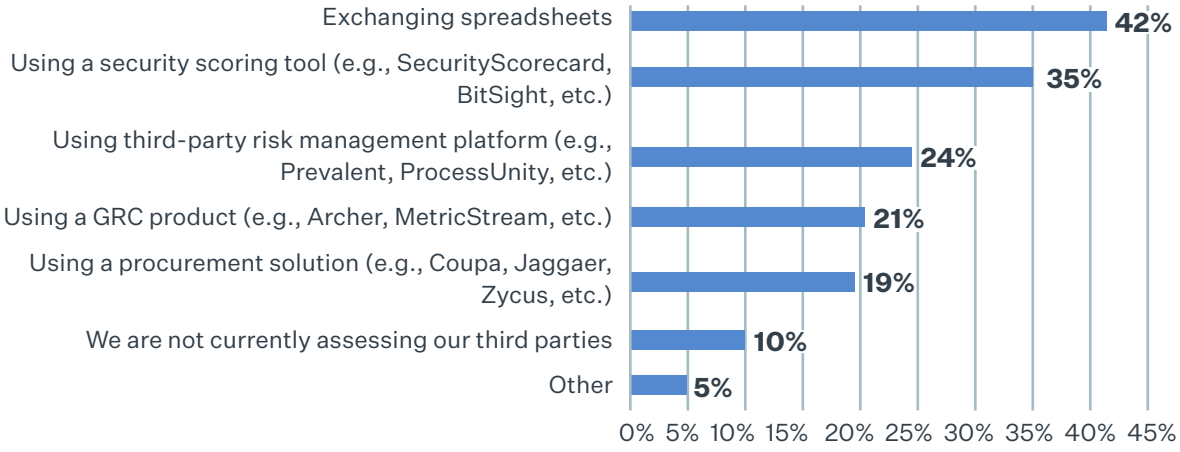
Visibility among key internal stakeholders



Finding #4: Third-Party Assessments Need to Modernize – and Outsourcing Leads the Way

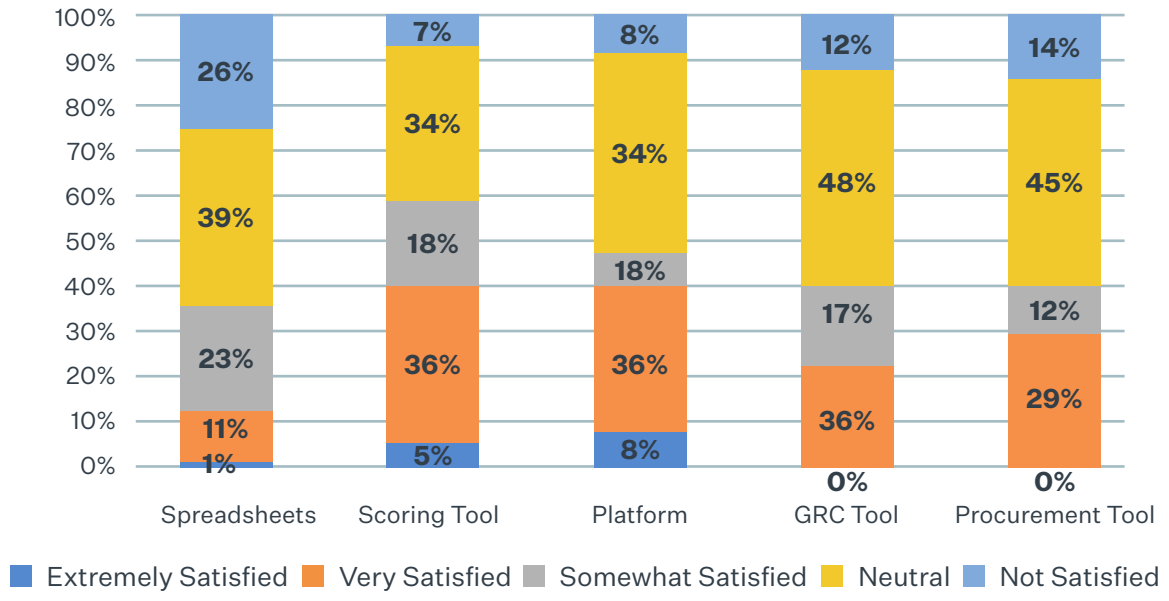
42% of respondents said they assess their third parties using spreadsheet-based questionnaires, slightly more than those using external risk scoring tools (35%).

How are you currently assessing third parties?



When asked about satisfaction with their current assessment method, respondents aren't thrilled, with almost no one feeling "extremely satisfied." **The spreadsheet method led the way in dissatisfaction at 26%.** Notably, the largest percentage of respondents (between 39% and 48%) rated their satisfaction as "neutral" across all methods. It's not encouraging when most respondents are just "meh" about their existing solutions!

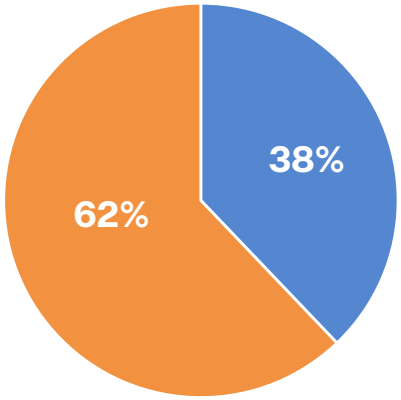
What is your level of satisfaction with the current assessment method?



Despite this relative level of dissatisfaction, only 38% of respondents are considering a new solution in the next 12 months.

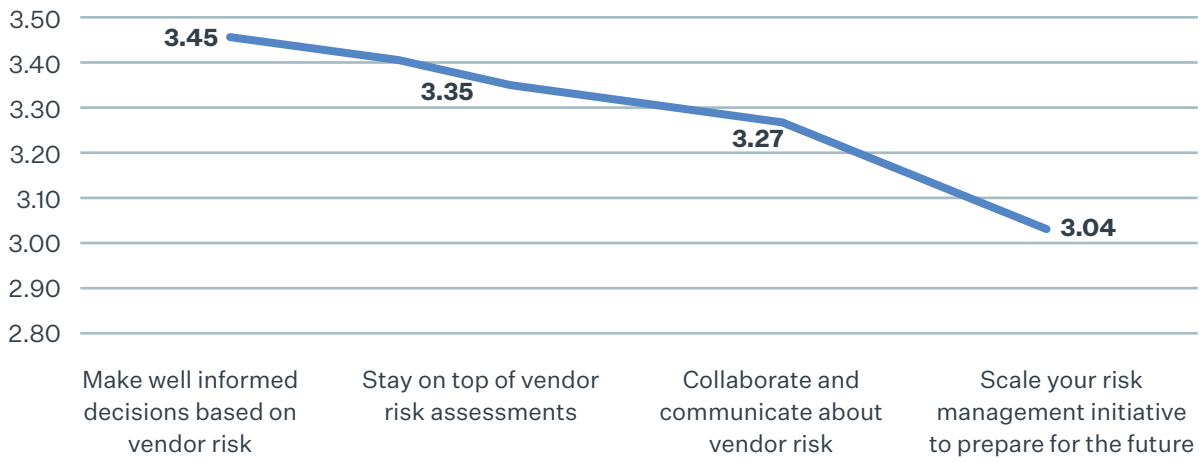
Are you planning to implement a new, or augment/replace an existing, TPRM solution in the next 12 months?

- Yes: **38%**
- No: **62%**



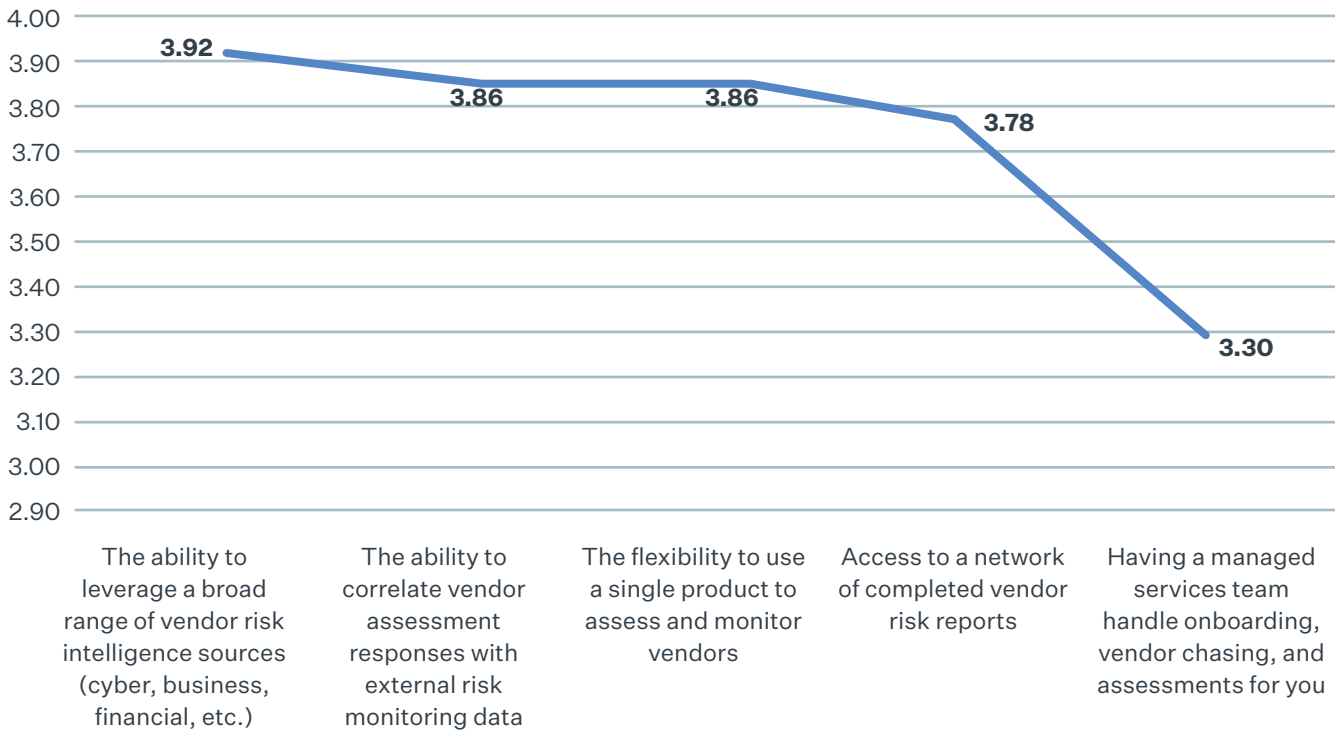
How confident were respondents in their TPRM programs? Respondents rated their program's outcomes between a 3 (scaling their program) and 3.5 (making well-informed decisions) on a scale of 1 (low) to 5 (high).

On a scale of 1 (low) to 5 (high) rate your organization's ability to...



Following this, organizations rated the ability to leverage a broad range of vendor risk intelligence sources (e.g., cyber, business, financial, etc.) as most important to their TPRM programs.

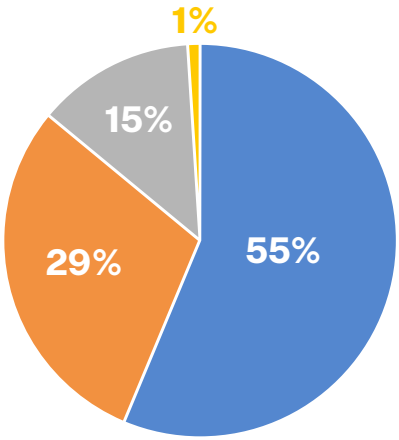
How important are the following aspects of a third-party risk management program? (1 low; 5 high)



When asked to describe their ideal approach to TPRM, **more than half of respondents (55%) preferred a hybrid approach** that balances internally managing some assessments and outsourcing others.

What is your ideal approach to conducting third-party risk assessments?

- A hybrid approach that enables management of some assessments and outsourcing of others: **55%**
- Use a product ourselves internally to assess third parties: **29%**
- Outsourcing third-party risk assessments to an outside managed service company: **15%**
- Other: **1%**



Recommendations

The results of this study demonstrate that IT security and business teams need to collaborate more closely to identify and mitigate risks at all stages of the third-party lifecycle. Here are our recommendations for unifying IT security and business for better outcomes from onboarding to offboarding.

Expand Assessments Beyond Cybersecurity

Third-party risk management isn't just a security and compliance problem. Many types of risks can impact an organization's ability to produce, manage, and distribute goods and services. For example, if a vendor declares bankruptcy, it may be unable to deliver on its contracts. Regulatory penalties, sanctions and lawsuits can impact strategy and a vendor's ability to execute against goals. Partnering with a company accused of bribery or corruption, or one with a poor environmental record, can be risky for your organization's reputation.

This requires security and procurement teams to work together to expand the scope of vendor risk assessments to include two areas on top of cybersecurity:

1. **Reputational intelligence** on legal actions and sanctions, executive leadership changes, politically exposed persons (PEPs), adverse media, state-owned enterprises, OFAC violations, and other indicators of potential cybersecurity or compliance problems.

2. **Financial information** including performance, turnover, profit and loss, shareholder funds, and other indicators.

Look for solutions that normalize monitoring data and correlate it against risk assessment findings to escalate potential risks and identify recommended remediations. Incorporating a broad range of risk intelligence sources will help security and procurement teams make better-informed decisions.

Bridge the Gap Between Business and IT

Disjointed approaches to assessing third-party risk leave gaps – and gaps introduce risk. You can unify IT security and business teams with a TPRM platform solution that provides a central source for everything from vendor profiles and contracts, to assessment results and compliance reports, to performance metrics and remediation logs. Having a single solution ensures that the entire organization is using the same data to make risk-based decisions.

Manage Risk at Every Step of the Third-Party Lifecycle

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.

1. Sourcing and Selection: You can accelerate pre-contract due diligence and avoid future headaches by subscribing to a vendor risk intelligence network. These networks provide on-demand access to libraries of completed, standardized vendor risk profiles. They offer a fast, efficient way to compare prospective vendors and identify risks without having to conduct a full assessment. Look for networks that also provide continuous monitoring of each vendor for real-time updates on potential security, reputational and financial issues.

2. Intake and Onboarding: With so many teams having a stake in third-party relationships, it can be tough to stay coordinated. A third-party risk management platform can enable IT, security, procurement, legal, compliance and other teams to collaborate on building comprehensive, centralized vendor profiles. Look for platforms that offer workflow rules to speed profile creation, automated updates with industry and business insights, and role-based access that gives everyone the information they need without compromising security. The best solutions also offer visual mapping capabilities that enable you to drill-down on each profile to uncover the 4th and Nth party relationships that make up your supply chain.

3. Inherent Risk Scoring: In this study, respondents reported having to manage an average of 2,400 third parties. If you have a large third-party ecosystem, then vendor profiling and tiering will be critical to prioritizing your ongoing risk assessments and other due diligence tasks – and this starts with inherent risk scoring. A good TPRM platform will include inherent risk assessment capabilities for quantifying and scoring third parties based on their risk levels before accounting for any specific controls. You can then use inherent risk scores to appropriately select and scope future assessment and monitoring activities for each vendor based on their potential risk to your business.

4. Vendor Risk Assessment: Periodic, questionnaire-based vendor risk assessments enable you to gather specific controls and compliance data from each of your vendors. However, the assessment process can be notoriously tedious and time-consuming – especially if email and spreadsheets are the only tools at your disposal. A good third-party risk management platform will automate the assessment process for you and offer access to standardized assessments (e.g., SIG and SIG Lite), industry-specific questionnaires, compliance questionnaires, and customization capabilities. Be sure to also evaluate the platform's ability to help you address identified risks, such as through remediation recommendations or workflow and task management capabilities.

5. Continuous Risk Monitoring: Even the best TPRM programs are usually only able to gather questionnaire-based risk assessments on an annual basis. That's why complementing your assessments with continuous monitoring is essential for staying on top of potential threats. Monitoring can also help you to validate assessment results by checking internally reported controls against external incidents affecting your vendors. The best monitoring solutions will not only provide cyber security intelligence (breaches, vulnerabilities, leaked credentials, etc.), but also business, financial and reputational insights (e.g., ABAC and ethics, diversity, ESG, Modern Slavery, etc.).

6. SLA and Performance Management: 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 reporting and document management capabilities. This is not only critical to internal reporting, but also can be a valuable tool in measuring adherence to vendor contracts, SLAs, KPI targets and compliance requirements. The results can inform ongoing negotiations with your business partners and ensure stronger, long-term business relationships.

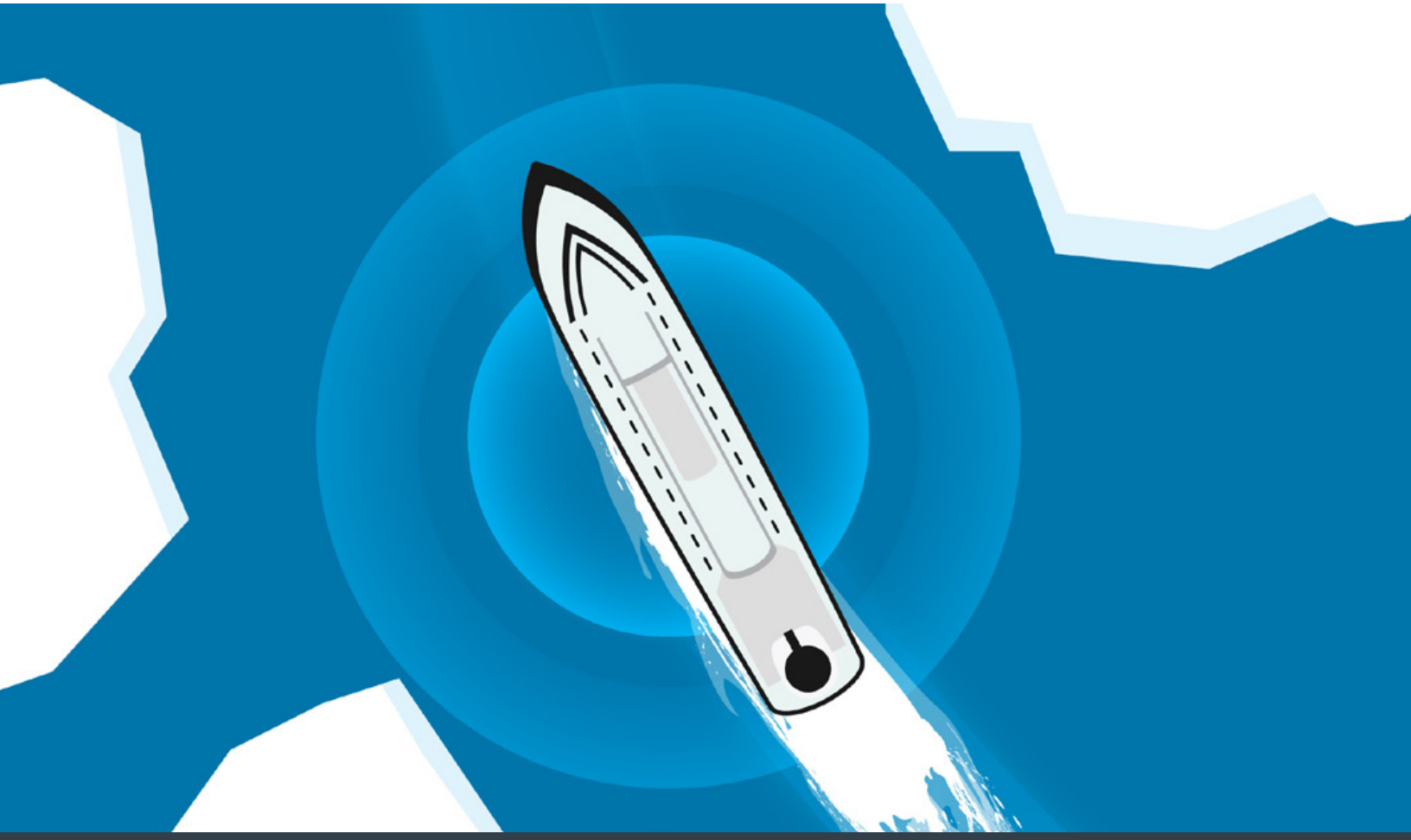
7. Offboarding and Termination: Offboarding is often overlooked when it comes to third-party risk management, however a lot can happen in the last days of a vendor relationship. Conducting a final risk assessment can validate that your systems and data are securely decommissioned, while also providing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

Outsource the Hard Stuff

The results of this study show that the preferred method for most organizations is to outsource on some level. Third-party risk management experts can manage the vendor lifecycle on your behalf – from onboarding vendors and collecting evidence, to reviewing assessments for completeness, identifying risks, and providing remediation guidance. As a result, you can safely navigate dangerous waters by efficiently scaling your TPRM program, reducing vendor risk, and simplifying compliance without burdening your internal staff.

Conclusion and Next Steps

Respondents to this year's study made it clear that their organizations are recognizing the importance of expanding third-party risk visibility beyond the usual cybersecurity factors. However, most are still trying to figure out how to bring together the right people, processes and solutions to achieve a more holistic understanding of third-party risk. If you're in a similar situation, then Prevalent can help.



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.

© 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. 04/21