riskrecon by Mastercard | Cyentia Institute

CYBERSECURITY PERSPECTIVES

The state of third-party risk management

SURVEY REPORT
MARCH 2024

Contents

Introduction

Welcome to the second study examining perceptions and practices in third-party risk management (TPRM). It's been a while since the last edition, which was conducted in the middle of a global pandemic in 2020. Business and technology paradigms have shifted since then, and it's high time we examined how TPRM programs have evolved with them.

One paradigm shift that's particularly relevant is the eroding barrier between "us" and "them" when it comes to managing cyber risk. The Security and Exchange Commission's (SEC) recent ruling is a perfect example, concluding that investors see no difference between a breach occurring in first vs. third-party systems when assessing the materiality of an cyber event.

It's not surprising, then, that our findings demonstrate TPRM has grown in strategic priority and scope. The stakes are higher too; supply chains are expanding and third-party breaches are much more common. But we also see evidence that TPRM teams are rising to meet the challenge. Ready to join them in that endeavor? Great—let's get started!

This survey was conducted by RiskRecon. Invitations were sent to contacts that participated in the prior State of TPRM study, attended relevant events, or who use RiskRecon's platform. Additionally, invites were sent to members of the Retail and Hospitality ISAC. This resulted in a sample of 112 confirmed responses.

Key findings

90%

of respondents consider TPRM a growing priority (up from 63% in 2020).

23%

Nearly a quarter of organizations experienced security incidents from a third-party (up from 9% in 2020).

57%

Over half of organizations say their TPRM program is adequately staffed.

x2

Twice as many firms manage 250+ vendors in 2023 (26% vs. 13.5% in 2020).

~20%

About 1 in 5 firms assess that at least half of their vendors could cause material harm.

↑45%

Organizations using security ratings services surged from 42% in 2020 to 61% in 2023.

4%

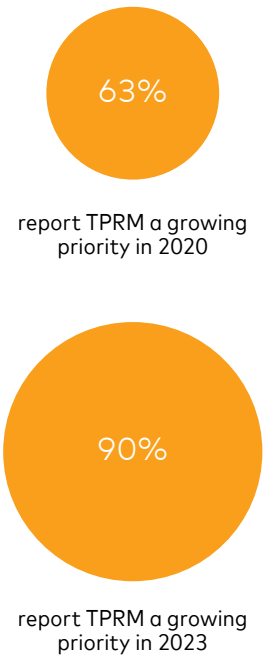
Questionnaires are getting longer but only 4% of respondents express high confidence that answers match reality.

89%

of TPRM programs assess non-cyber risks or will soon begin doing so.

TPRM program growth

Figure 1: Change in TPRM as a growing priority from 2020 to 2023 surveys



A key theme that emerged from the 2023 survey responses is the growing priority, scope, and size of TPRM programs compared to 2020. A larger percentage of respondents report that managing third-party risk is a priority and increasingly look to their TPRM programs to address a wider range of non-cyber risks.

TPRM increasing in priority

The management of third-party risk competes with many other cyber and non-cyber concerns in organizations today. Despite that fact, TPRM appears to be gaining traction in managerial circles. A full 90% of respondents consider TPRM a growing priority for their organizations. That's up from 63% when we inquired about this in 2020.

We can't help but wonder if this trend is at least partly attributable to a growing body of legislation emerging to address third-party risk. For example, the SEC recently adopted new rules governing the public disclosure of cyber events. The Final Rule mentions third-party risk 39 times and cites the increasing reliance on service providers as one of the primary reasons for the Rule's issuance.

89%

of TPRM programs assess non-cyber risks or will within 1 year.

TPRM expanding in scope

New evidence points to the scope of TPRM (finally) expanding beyond a largely compliance-driven function. Back in 2020, the major drivers for TPRM were regulatory compliance (62%), executive mandates (22%), and customer requirements (16%). Our recent survey shows little change for compliance (65%) and exec mandates (30%) but reveals a significant increase in respondents citing customer requirements (46%) as a reason for managing third-party risk.

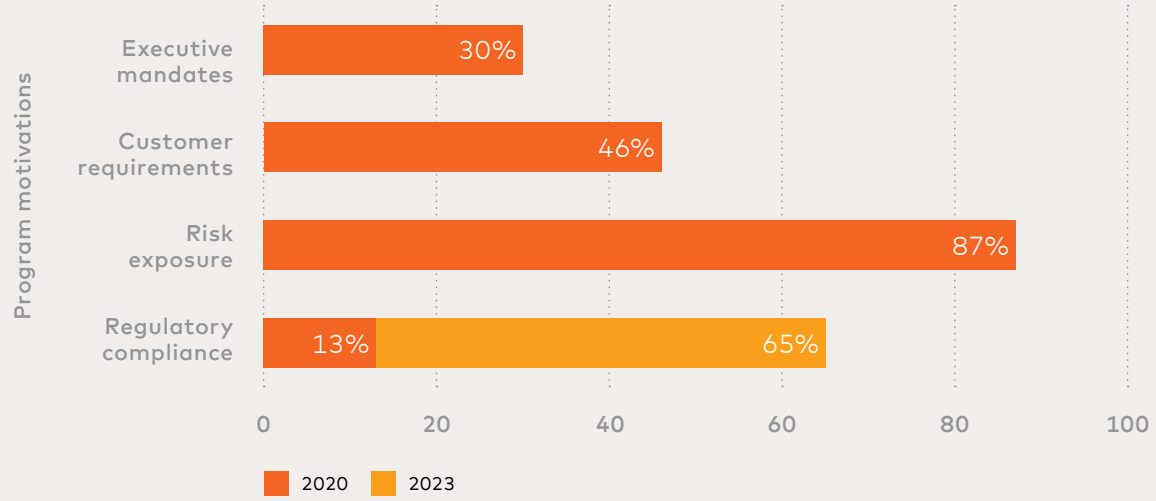
62% – 65%
Regulatory compliance

22% – 30%
Executive mandates

16% – 46%
Customer requirements

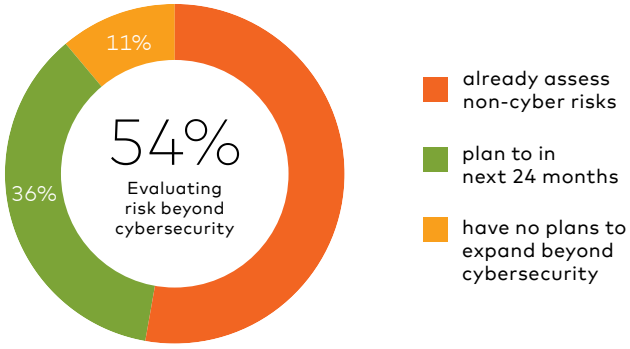
The primary motive of modern TPRM programs, however, is reducing risk exposure (87%). This wasn't included as an option in the prior survey, so we don't have that data point for comparison. But we're glad to see that the "R" in TPRM is now seen as the primary benefit. TPCM (Compliance) just doesn't have the same ring to it.

Figure 2: Motivation for TPRM programs



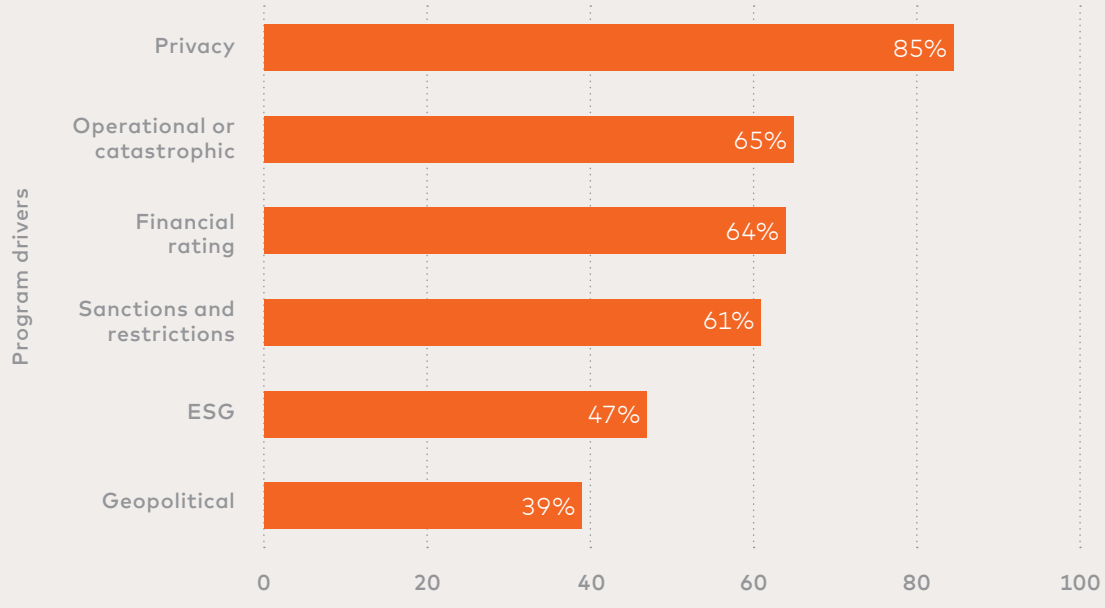
We also asked respondents if the scope of their TPRM program was expanding beyond cyber-specific risks. A slim majority (54%) claim their programs already assess non-cyber risks with another 36% planning to do so in the next 24 months. Only 11% say their organizations have no plans to expand beyond cybersecurity in the foreseeable future.

Figure 3: Scope of TPRM programs beyond cyber risk



Privacy was cited as the most common non-cyber risk factor considered within the scope of TPRM programs (85% of respondents). Other factors include operational risk (65%), financial ratings (64%), regulatory sanctions (61%), environmental and social governance (47%), geopolitical risk (39%). These results demonstrate that TPRM is expanding its horizons, which is important because cybersecurity is increasingly intertwined with the other risks identified here.

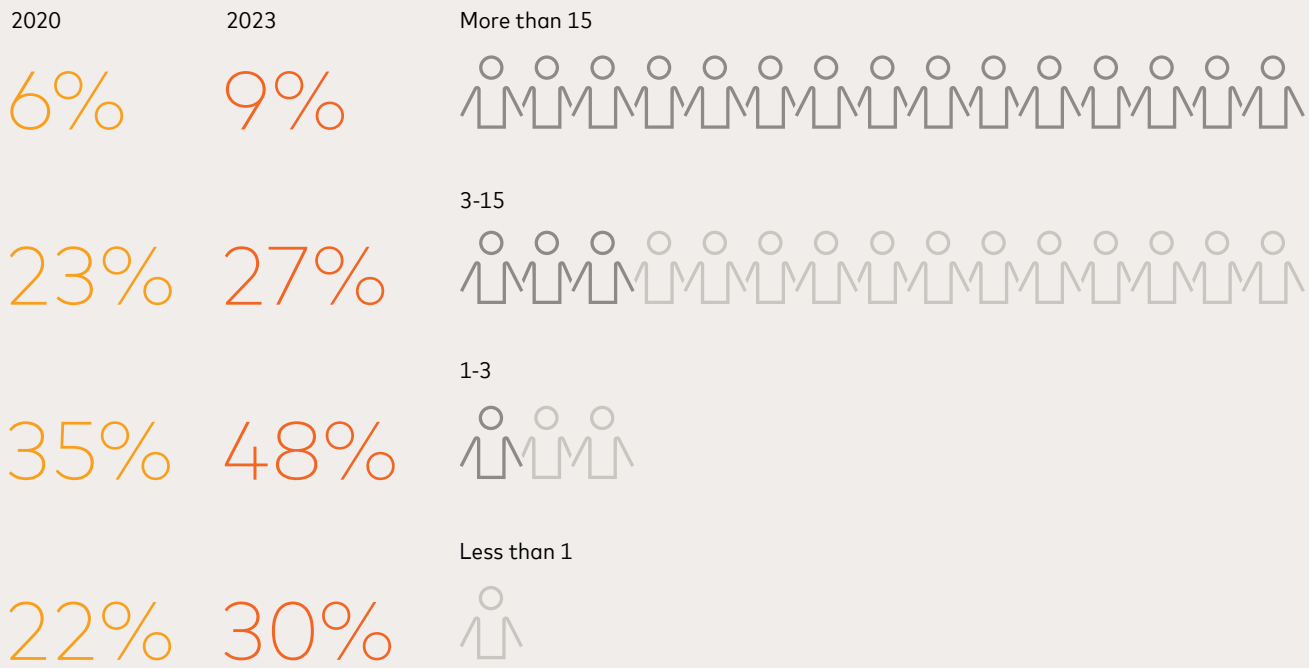
Figure 4: Most commonly reported non-cybersecurity concerns of TPRM



TPRM programs growing in size

Possibly in response to increasing priority and scope, firms appear to be allocating more resources to TPRM. The number of organizations with less than one full-time equivalent (FTE) staff member dedicated to managing third-party risk ebbed from 30% in 2020 to 22% in 2023. That was accompanied by a one-third (35% to 48%) increase in programs reporting one to three FTEs. Curiously, we see fewer TPRM programs with more than 15 people this time around.

Figure 5: Number of FTE staff supporting TPRM programs

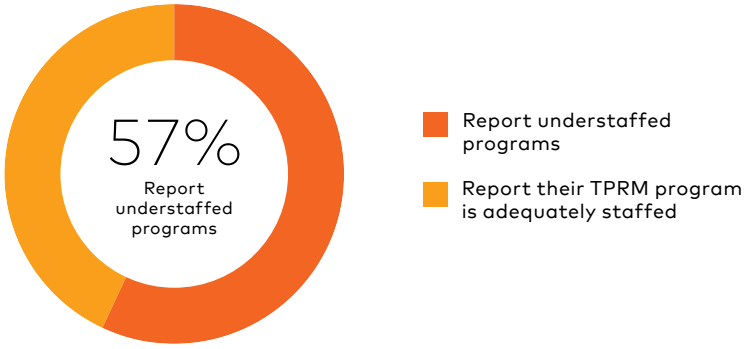


43%

claim their TPRM program is adequately staffed.

Despite the uptick in dedicated FTEs, staffing levels remain a concern. Less than half (43%) of respondents say their TPRM program is adequately staffed. Furthermore, this notion of being shorthanded isn't going away—our 2020 survey showed the exact same percentage.

Figure 6: Sufficiency of TPRM program staffing



We see several reasons behind this sense of staffing inadequacy. The increased scope of TPRM is likely one of them. Team size has edged up, but so has the scope of their responsibilities. And as the next section will show, the number of third parties—and security incidents tied to them—are growing as well.

Vendor reliance and risk

26%

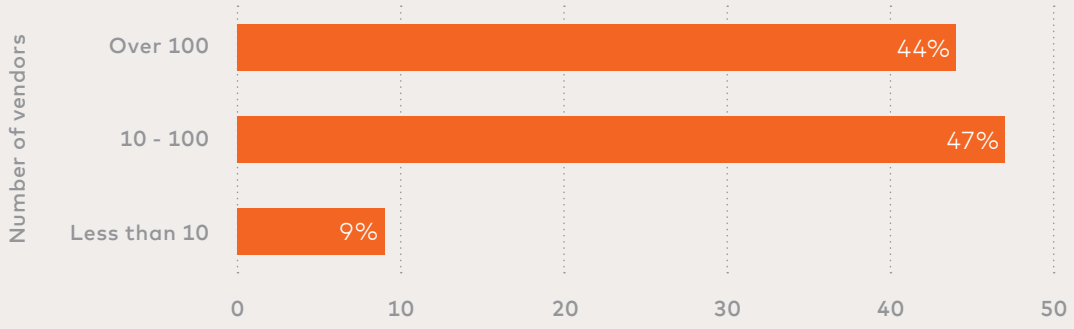
Double the number of TPRM programs managing at least 250 vendors in 2023 (26% vs. 13.5% in 2020).

We asked a series of questions to better understand the size and composition of third-party portfolios being managed by the organizations in our sample. We learned that they're contending with more vendors, many of those vendors represent material risk, and third-party incidents have increased. That's a challenging trio of traits, so let's examine them more closely.

Reliant on more vendors

Participants report an increase in the number of vendors they're assessing each year. Double the number of TPRM programs managing at least 250 vendors in 2023 (26% vs. 13.5% in 2020). Over two-thirds of firms have 50 or more vendors in their portfolio, compared to 41% in 2020. And the percentage of TPRM teams managing less than 10 vendors stands at 9%—well below the 25% set in 2020.

Figure 7: Number of third parties assessed each year



All this points to the fact that organizations are increasingly reliant on third parties to support their core products and services. This growing reliance translates into larger vendor portfolios that further burden already-strained TPRM teams.

1/5

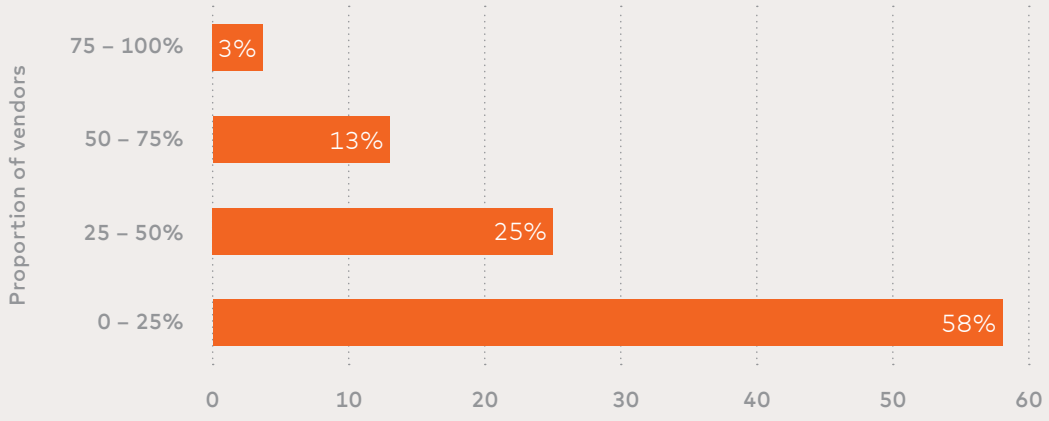
Over half of 1 in 5 firm's third-party vendors could cause material harm.

Vendors represent material risk

Not only do TPRM programs have more vendors to manage, but those vendors represent higher levels of risk. This trend is especially important to monitor in light of the aforementioned SEC Rule. We asked a couple of questions that each targeted a different angle on this topic.

First, we asked respondents what proportion of third parties fall in their most critical risk category. About 40% of organizations say it's a small minority (less than 20%). Only ~10% of firms categorize a super-majority (80%+) of their vendors as critical.

Figure 8: Proportion of third parties that could cause material harm



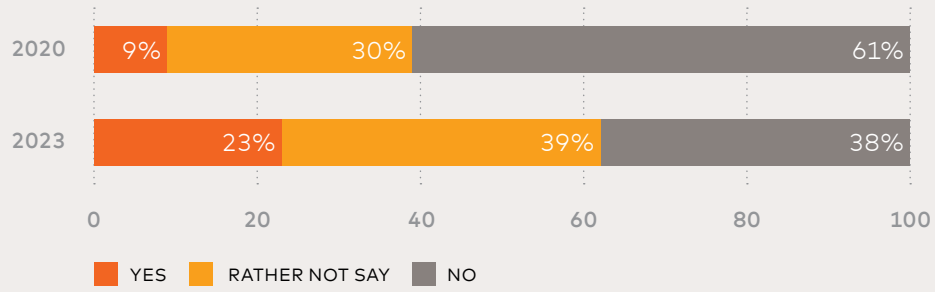
We also asked participants to estimate the percentage of vendors that could cause major operational disruptions resulting in material harm to their organizations. A little less than one in five firms assert that over half of their third-party vendors could trigger such impacts. That's actually a slightly lower proportion than in our 2020 survey, but keep in mind vendor portfolios have grown since then.

More third-party incidents

When asked back in 2020, only 9% of respondents reported that their organizations suffered a security incident related to a third party. That now stands at a much-increased 23% in our latest survey. Furthermore, a much lower proportion were confident that their firms did NOT have a vendor-related incident (39% in 2023 vs. 61% in 2020).

Plot of 2020 with a corresponding plot of 2023 below:

Figure 9: Has your organization suffered a security breach from a third party?



The true prevalence of third-party breaches, however, may be much higher than what's reported here. In a sample of about 1,000 organizations using RiskRecon to monitor third parties, 100% of them had at least one firm in their portfolio with a detected breach in the preceding 36 months. You can read more about that analysis in our Balancing Third-Party Risk report.

"We are not exempting registrants from providing disclosures regarding cybersecurity incidents on third-party systems they use, nor are we providing a safe harbor for information disclosed about third-party systems. While we appreciate the commenters' concerns about a registrant's reduced control over such systems, we note the centrality of the materiality determination: whether an incident is material is not contingent on where the relevant electronic systems reside or who owns them. In other words, we do not believe a reasonable investor would view a significant breach of a registrant's data as immaterial merely because the data were housed on a third-party system, especially as companies increasingly rely on third-party cloud services that may place their data out of their immediate control."

– SEC Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Third-party assessments

61%

The proportion of organizations using such services surged from 42% in 2020 to 61% in 2023.

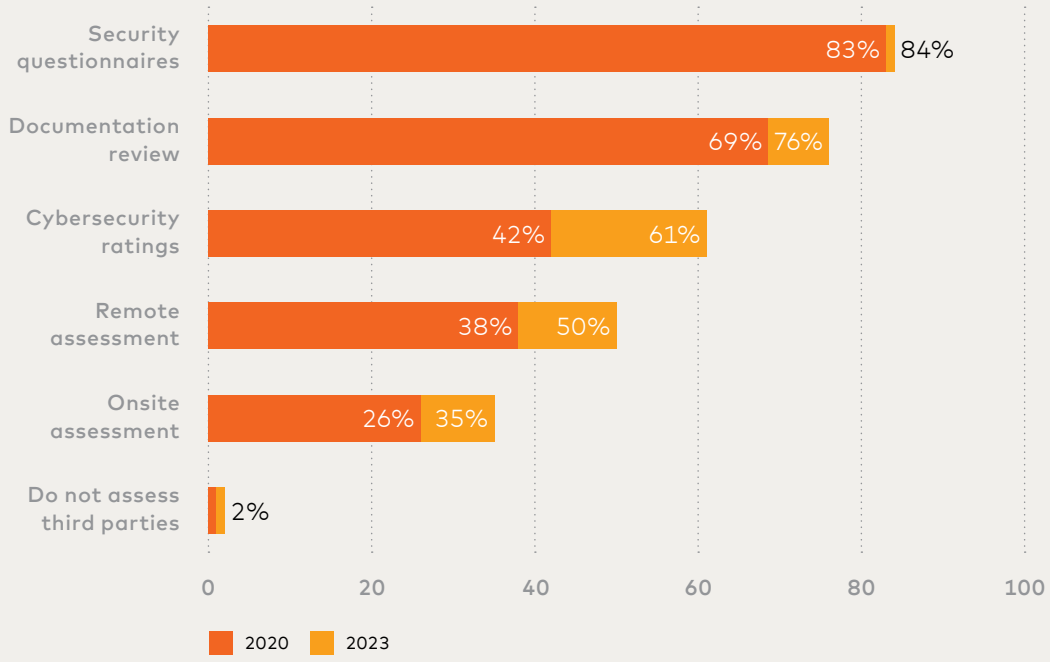
Respondents indicate that traditional security assessment methods such as questionnaires are still a live and well. At the same time, there are signs that more TPRM programs are improving efficiency by using security ratings solutions. We also see limitations in organizational authority to take actions to manage third-party risk.

A surge in security ratings

Security questionnaires remain the most popular method of assessing third-party risk and show the same usage levels as we saw back in 2020. Documentation reviews have become somewhat more common, while both remote and onsite assessments are less so.

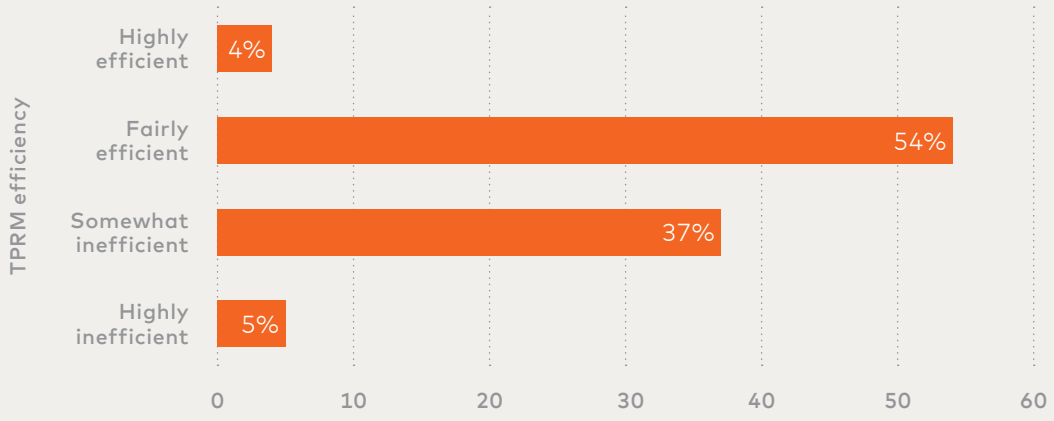
The largest change was in the use of cybersecurity ratings. The proportion of organizations using such services surged from 42% in 2020 to 61% in 2023. We hypothesize this is a response to trends highlighted earlier in this report, such as larger number of vendors, increased scope of TPRM programs, and strained staffing levels. Security ratings offer improved scalability and efficiency.

Figure 10: Methods used to assess third parties



Supporting evidence for this hypothesis comes via another question in which we asked respondents whether they consider their TPRM program's activities to be efficient. Overall, 57% answered in the affirmative. A scant 4% rate themselves as highly efficient. Organizations that use security ratings, however, were more likely to report efficient programs than those that don't use ratings services (63% vs 48%).

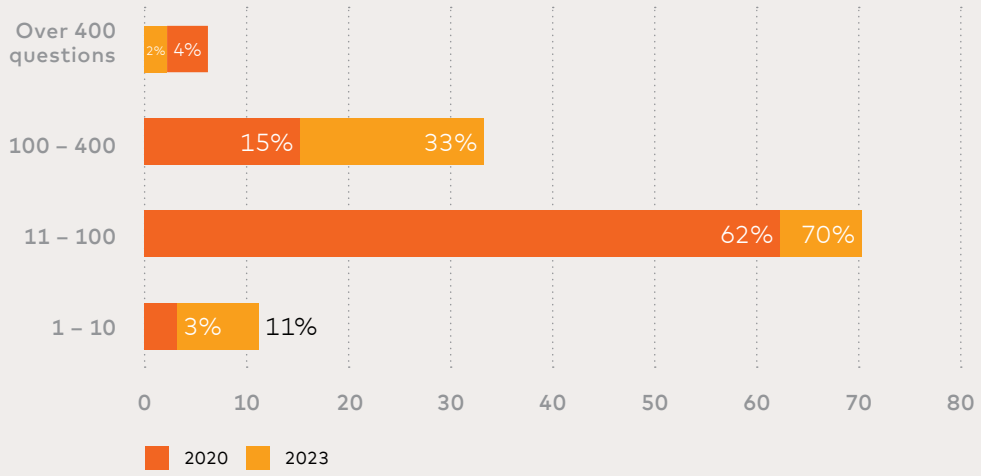
Figure 11: Respondents' rating of TPRM program efficiency



Questionnaires longer, customized

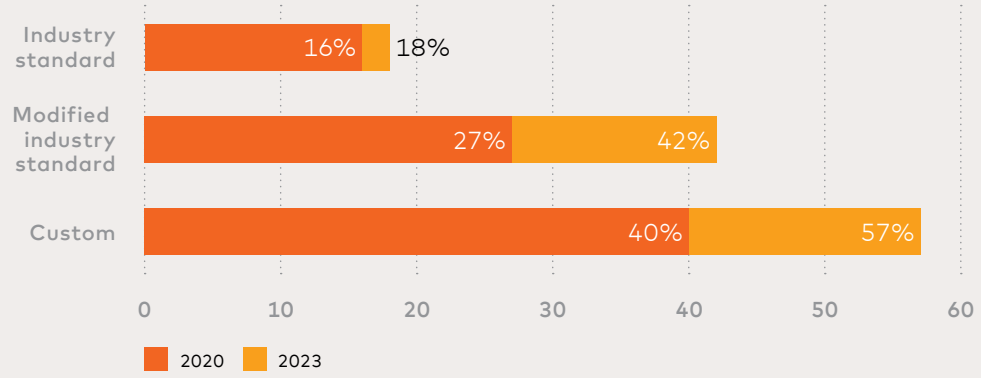
While usage of questionnaires remains steady, the number of questions being asked is growing. The proportion of TPRM programs that include at least 100 questions in their vendor surveys has grown from 19% in 2020 to 35% in 2023. Only 3% take the "short and sweet" approach of asking 10 questions or less.

Figure 12: Number of questions in third-party security questionnaire



A small minority of organizations base their vendor risk assessment questionnaires fully on industry standards (e.g., Shared Assessments SIG), which hasn't changed since 2020. Use of custom-built questionnaires, on the other hand, has bumped up substantially. That growth appears to be fueled by a shift away from modified industry standards.

Figure 13: Source of security questionnaires used by respondents



30%

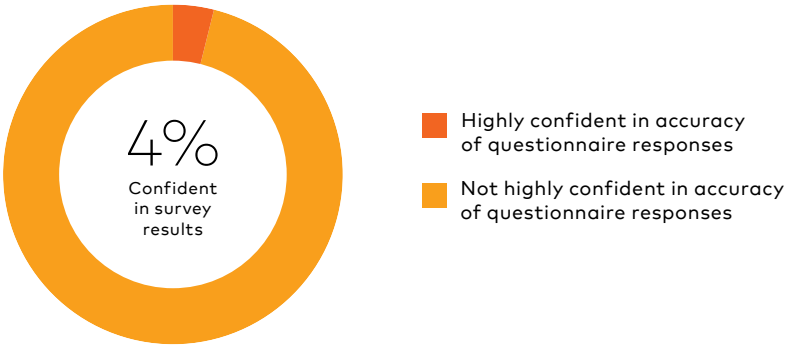
of firms report that at least 75% of their vendors passed their assessment.

We find this shift toward fully customized questionnaires rather curious in light of the prevailing trends in the TPRM space, which would seem to favor standardization (e.g., more vendors, executive visibility, increased regulation). Then again, perhaps it's precisely those trends that necessitate more tailored information gathering related to vendor risk.

Firms questioning questionnaires

Despite questionnaires being longer and more customized, doubts prevail about their validity. Only 4% of respondents say they're highly confident that vendors are actually meeting security requirements based on their questionnaire responses. That's down from 14% in 2020. This position seems justified, as 80% of firms report that inaccurate answers are not an uncommon occurrence.

Figure 14: Percent of respondents highly confident in the accuracy of questionnaire responses



While the fact that most firms discover inaccuracies in vendors' responses is unfortunate, there may be a silver lining. About 30% of organizations report that the vast majority of their vendors (at least 75%) pass their assessment questionnaire without flagging any major issues. When asked back in 2020, a much larger 78% of firms reported the same pass rate. We see less permissiveness as a good thing for TPRM. As journalist Sydney Harris once wrote, "*skepticism is not an end in itself; it is a tool for the discovery of truths*."

Figure 15: Percent of third parties that pass assessment without required remediation

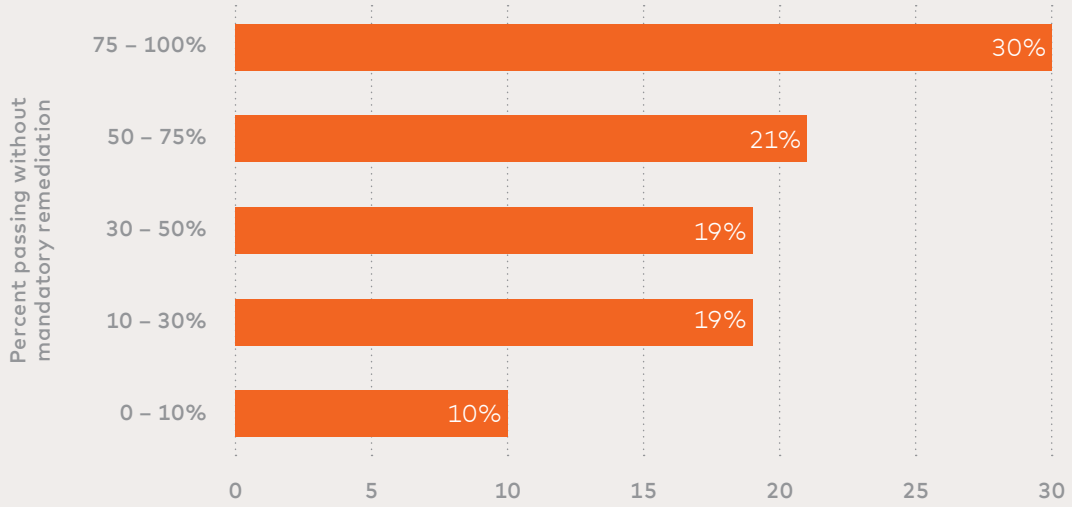


Figure 16: Percent of TPRM programs having various levels of authority

Programs lacking authority

Fewer TPRM programs are giving the green light to vendors without some level of remediation, which suggests they've gained more authority to act. That's a positive development for managing third-party risk. But we also see some signs pointing to limitations in that authority.

Just over 3 in 10 organizations make a habit of reducing the scope of TPRM assessments for vendors with a strong security track record. That's roughly equal to our 2020 survey (38%). This seems like a missed opportunity to adopt a risk-based approach that could create efficiencies by diverting focus to poor performers.

Almost half of TPRM programs claim to have the authority to block the onboarding of new vendors based on security concerns revealed during assessments. But a much lower proportion (28%) say they're able to terminate existing vendors over security concerns. Ideally, those should be in better alignment, since they're two sides of the same TPRM coin.

And finally, nearly 60% of programs report having the authority to require vendors to implement additional security controls. While that represents the majority, it leaves 40% of teams without the ability to use a tool that would seem fundamental to managing risk.

One can't help but wonder if such limitations contribute to the rising frequency of third-party incidents documented earlier in this report. Time (and our next survey) will tell.

A more secure future

Areas for improvement included:

- Accuracy of scores to reflect risk posture
- Transparency of models and algorithms
- Integration with adjacent security solutions
- Explanation and actionability of ratings

Not long after the publication of our first study, Forrester released a Wave on Cybersecurity Risk Ratings Platforms. It assessed that then-current solutions needed to mature in order to meet the demands of the enterprise market.

This new study makes it clear that enterprise demands have certainly continued to grow since then. Organizations place greater strategic priority on TPRM to contribute to a widening scope of enterprise risk that extends beyond cybersecurity. It's also clear from these results that supply chains are expanding as is the need to efficiently assess risk across those business relationships. Respondents tell us they're increasingly relying on automated assessments and risk ratings to meet that demand.

The big question is whether cybersecurity risk ratings solutions have risen to the occasion. We're biased on this matter, of course, but can say with all sincerity that our own approach to the shortcomings identified above has matured substantially in the intervening years. It's had to; customers won't tolerate stagnation when their reputations are on the line. Their requirements are our roadmap, many of which echo themes gathered from respondents of this study.

Is your organization ready to take the next step in third-party risk ratings? There's no time like the present. Creating a RiskRecon account to monitor your supply chain is free to try for 30 days. What's included in the offer?

- Detailed assessment of your own IT assets
- Security ratings and summary assessment of up to 50 vendors
- Full access to RiskRecon Technical Support
- A risk-prioritized view into your vendor ecosystem with our vulnerability matrix
- Superior data accuracy (over 99% – which drastically reduces false positives)

Register to get insights into your supply chain at: https://www.riskrecon.com/know-your-portfolio.

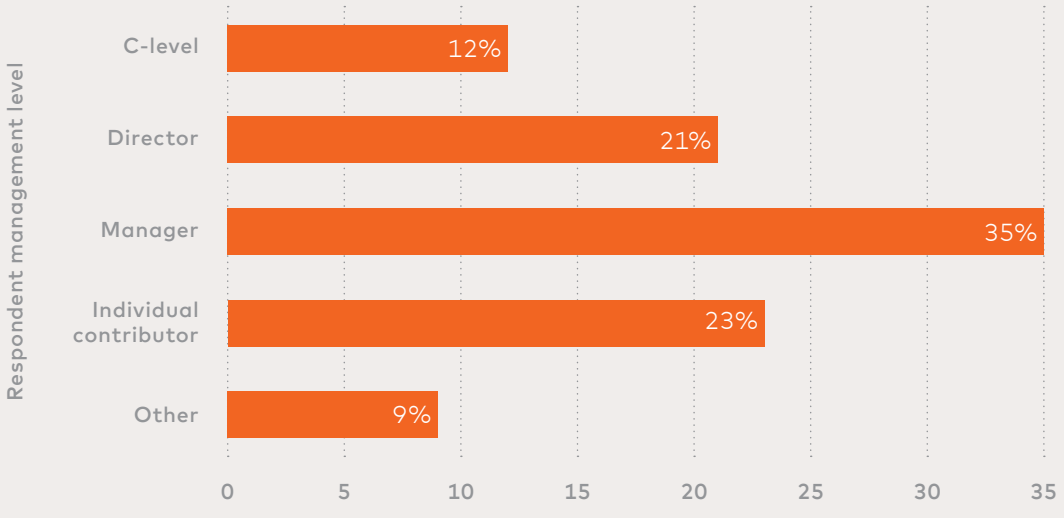
Appendix A

Survey firmographics

This survey was conducted by RiskRecon. Invitations were sent to contacts that participated in the prior State of TPRM study, attended relevant events, or who use RiskRecon's platform. Additionally, invites were sent to members of the Retail and Hospitality ISAC. This resulted in a sample of 112 confirmed responses.

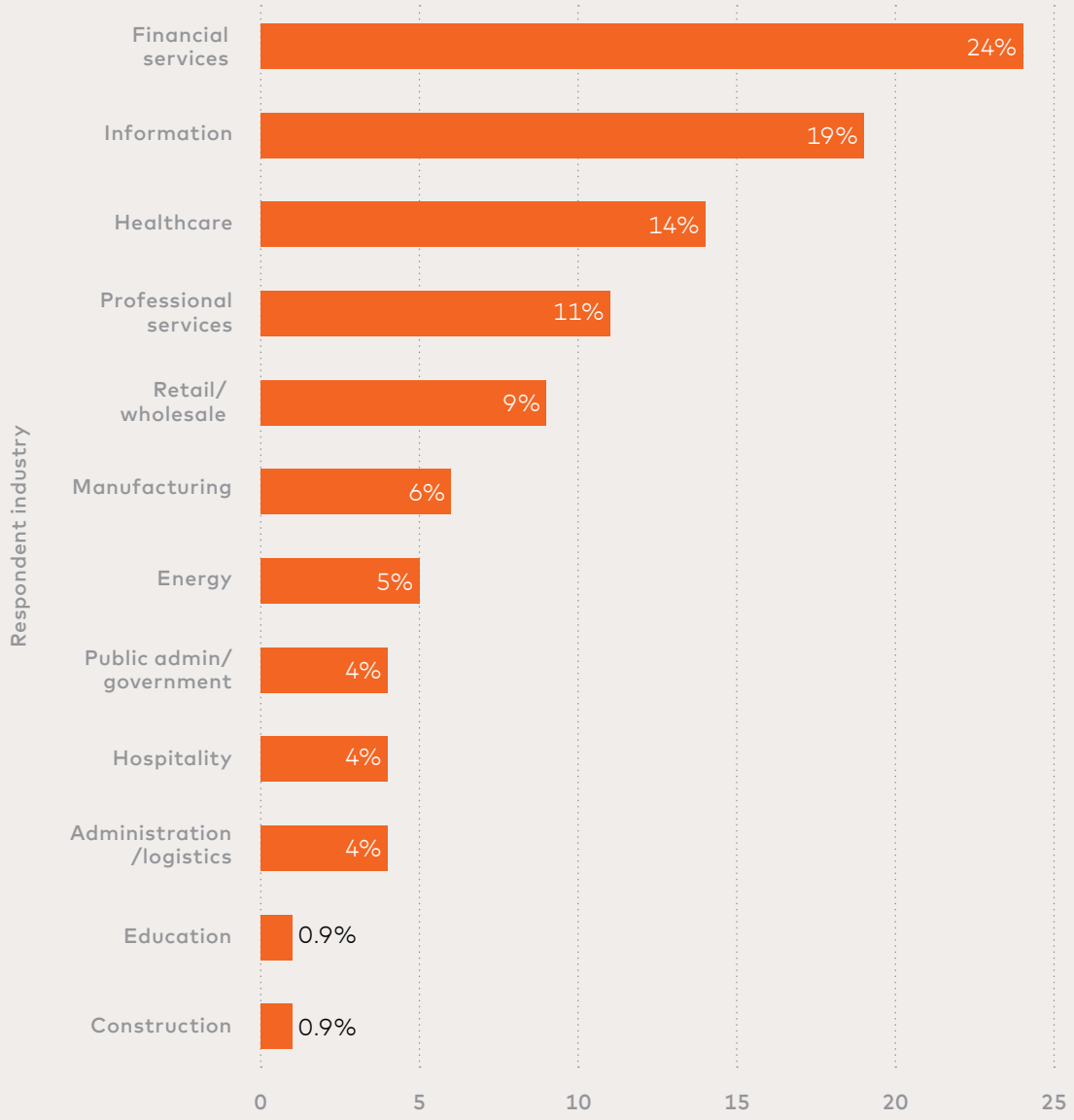
Respondents represented all rungs on the corporate ladder. Not surprisingly, the majority came from the bottom half of the ladder, including individual contributors (23%) and managers (35%). Directors (21%) and C-level executives (12%) account for nearly a third of all responses.

Figure 17: Management level of survey respondents



The organizations represented by these respondents span a diverse range of industries. The financial services sector tallied the most responses (24%), but information (19%), healthcare (14%), and professional services (11%) all had at least a 10% share.

Figure 18: Industry make up of survey respondents



We also had the pleasure of hearing from organizations of all sizes. Per Figure 19, we had about the same share of responses from smaller (<1,000 employees) and midsize (1,000 to 10,000) firms. Large enterprises with staff exceeding 10,000 represent about a quarter of respondents.

Figure 19: Distribution of respondents firm size