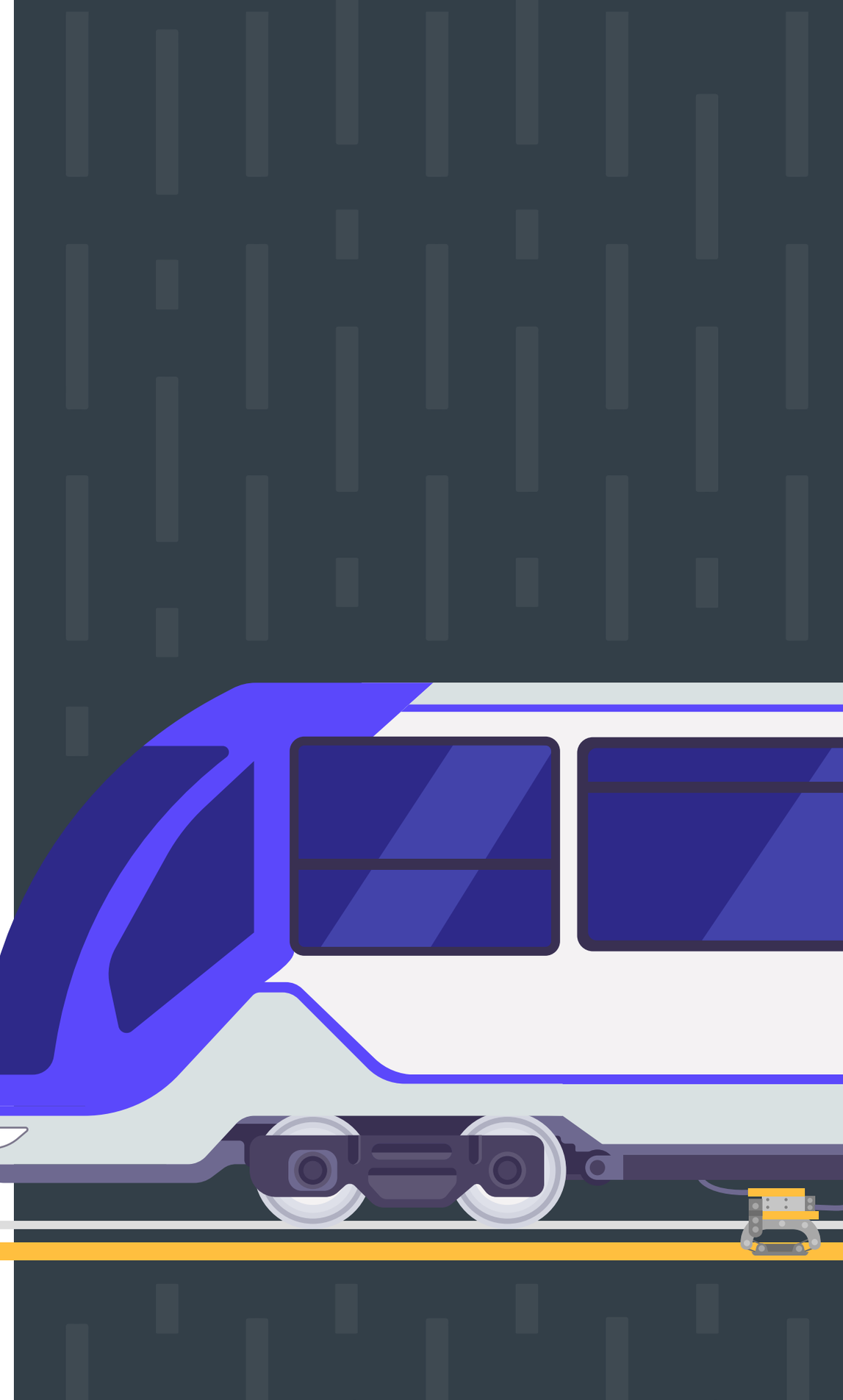
Prevalent™

SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

The 2020 Third-Party Risk Management Study

The 3rd Rail of Security & Compliance



Introduction

In February 2020, Prevalent and Shared Assessments partnered together to study current trends, challenges and initiatives impacting third-party risk practitioners.

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.

Respondents to the study were leaders and decision-makers in third-party risk.

Prevalent™

SFG SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

Summary

In today's business world, outsourcing key business functions is unavoidable. However, vendors have become the third rail of security and compliance. They come with significant risks which, if ignored, can lead your organization down a dangerous path.

The results of this study were both illuminating and shocking. The data suggests:

Lack of process is damaging third-party program effectiveness:

Compliance (particularly meeting data protection requirements such as GDPR) dominate project drivers, yet organizations lack the resources (budget) and processes to assess even their top-tier vendors, with most assessments taking more than a month to complete.

Third-party risk management is a team sport:

Compliance and cybersecurity teams aren't the only ones necessary to contribute to a mature program; you also need contributors who can assess and interpret business and financial risks. With resourcing a challenge and continuing lack of confidence in programs, it will be difficult to operate in a silo.

Lack of confidence in the program inhibits results:

54% of organizations have some meaningful experience in conducting third-party risk assessments, yet only 10% are extremely confident in their programs.

Significant consequences:

76% of respondents said that they experienced one or more issues that impacted vendor performance, 74% indicated operational issues, and 55% indicated a compliance violation in the last two years.

Few are happy with their existing toolset:

Satisfaction levels among existing tools hovers in the 50% range, and weighted average of satisfaction caps out at 3.8/5.0. GRC tools have an especially long way to go with a 41% satisfaction rate.

IRM – a way out?:

42% of respondents indicate that they will invest in IRM in the next year, yet they're concerned about limited resources/staffing/expertise, no real-time awareness of changes, and no integration with other tools used for vendor management or risk management. Since Digital Transformation is also a driver, it's important for organizations to determine if a general-purpose IRM has the flexibility to meet needs, compared to a purpose-built TPRM assessment platform.

Drivers

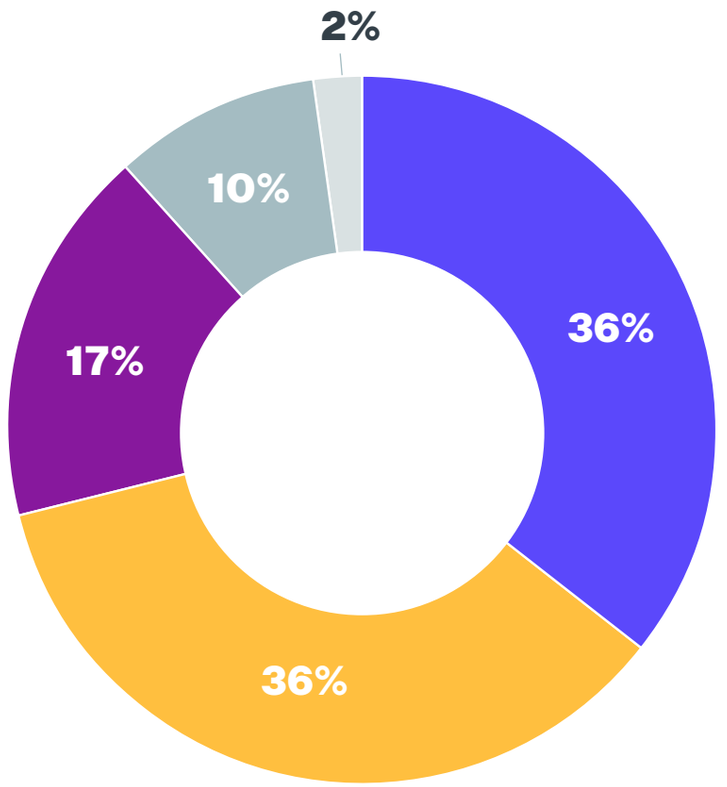
Finding #1:

Compliance and Cyber Risks Drive Nearly Three-Fourths of All Third-Party Risk Management Programs

Unsurprisingly, respondents were evenly split on why they perform third-party risk assessments with 36% saying they are required to by specific regulatory, industry framework or data privacy requirements, and 36% needing to ensure that third parties do not introduce cyber risks to their businesses. Efficiency and risk management are also important drivers, but ultimately a mature third-party risk management program provides visibility into compliance and cyber risk status so organizations can make better-informed decisions.

Which statement most accurately describes the objectives of your third-party risk management program?

- We are required to report against specific regulatory, industry framework, or data privacy requirements.
- We have to ensure that our third parties do not introduce cyber risks to our business that could negatively impact us.
- We have to improve the process of assessing and evaluating vendors to take less time and resources.
- We are driven by risk-based intelligence.
- Other



Drivers

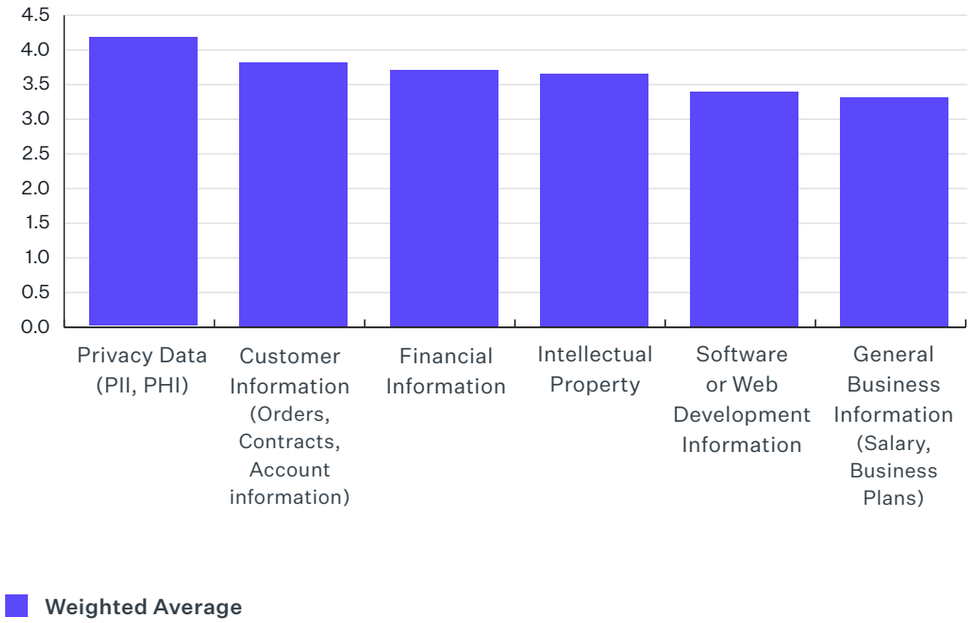
Finding #2:

Protecting Private Data – and Meeting GDPR Requirements – Dominate Third-Party Risk Concerns

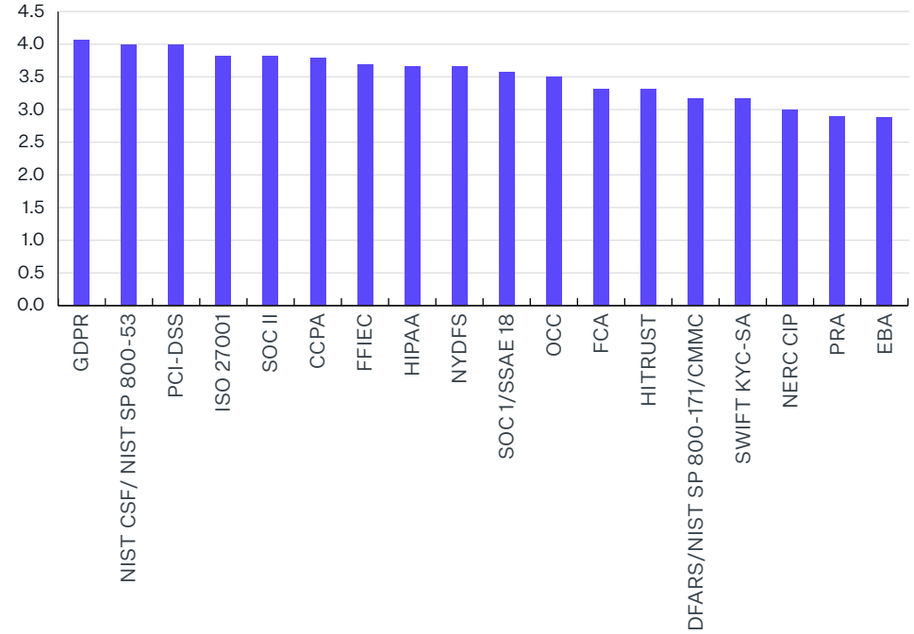
Expanding on what's driving their programs, respondents are most concerned about protecting privacy-related data (e.g., PII, PHI), with 51% classifying that data at an Extremely High Risk of third-party exposure. In fact, privacy data had the highest weighted risk average of all data types referenced in the study at 4.2/5.0.

This correlates to the fact that, when asked which regulations or industry frameworks were most important to their organizations, respondents assigned GDPR the highest weighted average at 4.1/5.0 out of all regulations mentioned. (Note: NIST, PCI, SOC 2, ISO and CCPA rounded out the top compliance mandates.)

Rate the risk exposure for each of these kinds of data if there is a lack of proper control over third parties:



Rate the importance of the following regulations/ industry frameworks to your organization:



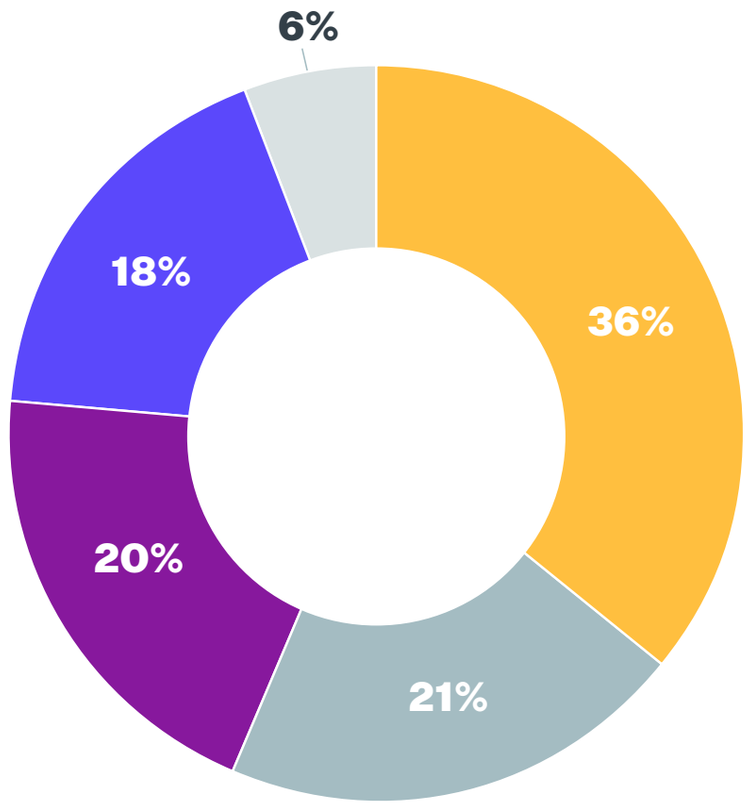
Challenges

Finding #3:
Third-Party Risk Management Isn't Mature Enough to Handle the Challenges

The study showed that 54% of respondents said their organizations have been conducting third-party risk assessments for less than 5 years. Further, only 10% of respondents are driven by risk-based intelligence (see Finding #1 – "Compliance and cyber risks drive nearly three-fourths of all third-party risk management programs" above). And finally, in one of the most telling statistics that emerged from the study, **only 10% of respondents are Extremely Confident in their third-party risk management programs.** Third-party risk is still a relatively new discipline that is not overly reliant on risk-based metrics yet and features a low level of program confidence among practitioners – all indicators of a less mature program.

How long has your organization been performing third-party risk assessments?

- 0-2 years
- 3-5 years
- 6-9 years
- 10 or more years
- We have not yet begun performing third-party risk assessments.



Challenges

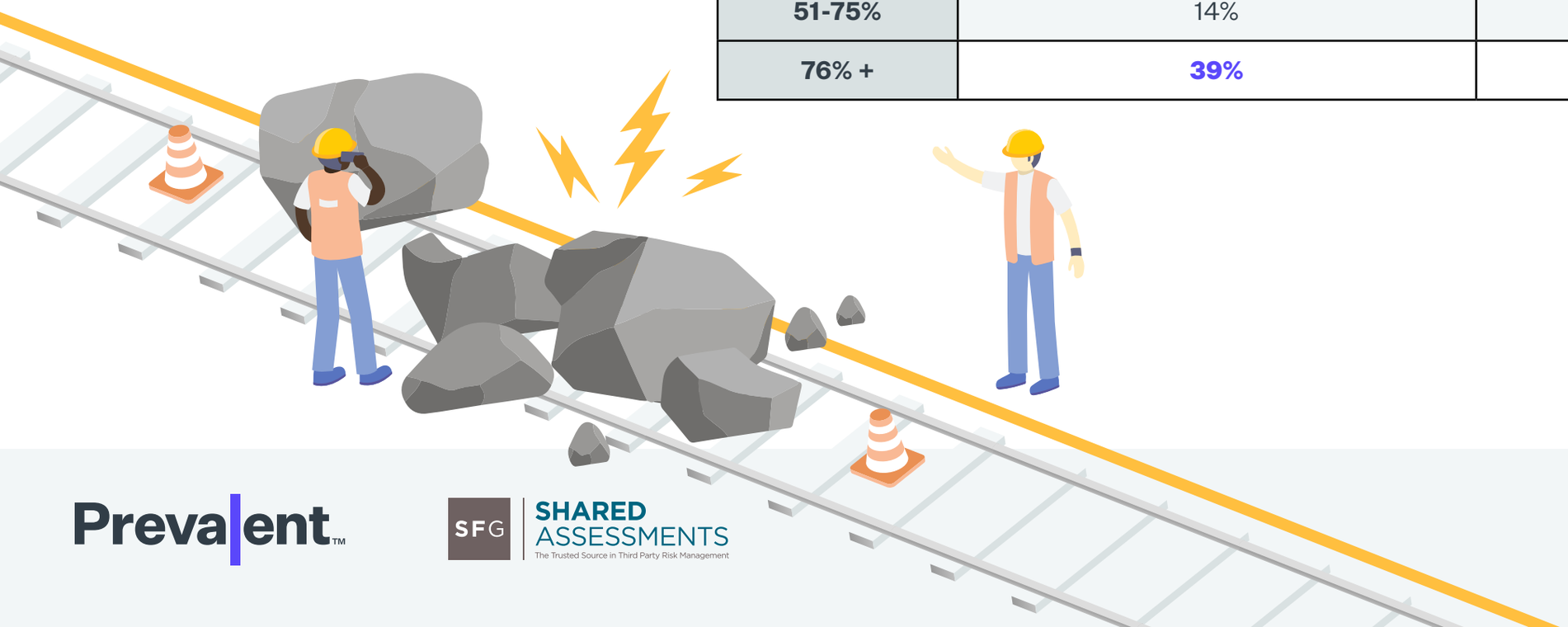
Finding #4:
… Especially When Organizations are Not Even Assessing Enough of Their Top Tier Vendors?

It's no wonder that practitioners aren't more exceedingly confident in their programs. Only 39% are assessing more than three-fourths of those top-tier vendors – and 66% say they *should be* assessing more than three-fourths of their top tier vendors.

39% are assessing more than three-fourths of those top tier vendors

66% should be assessing more than three-fourths of those top tier vendors

Share of Top-Tier Vendors	Percent of Respondents Who Are Currently Assessing	Percent of Respondents Who Think They Should Be Assessing
1-10%	17%	7%
11-25%	15%	8%
26-50%	16%	9%
51-75%	14%	9%
76% +	**39%**	**66%**



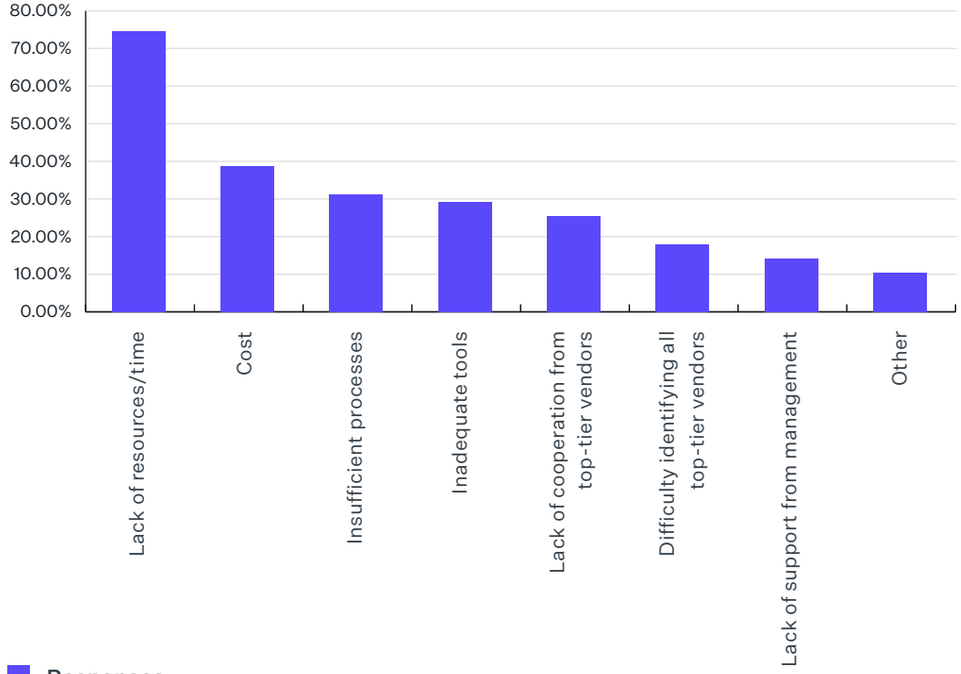
Challenges

Finding #5:

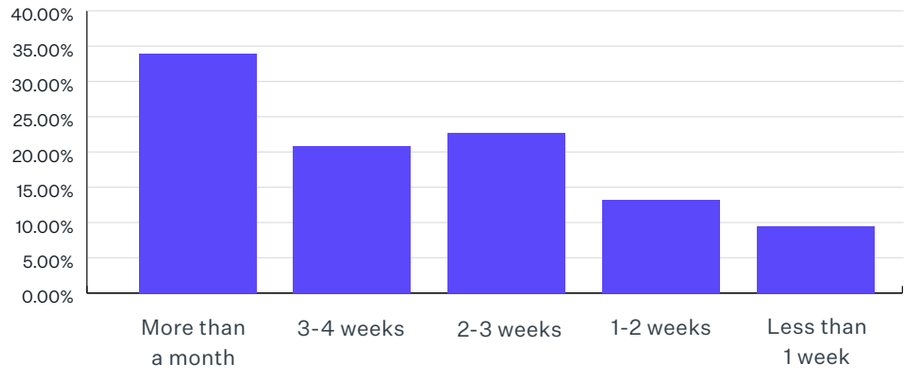
Costs, Resources and Lack of Process are Inhibitors to Success

Lack of resources (74%), cost (39%) and insufficient processes (32%) are keeping respondents from assessing all their top-tier vendors. This is not surprising, since 34% of respondents indicated that it takes more than a month to complete an assessment of their top-tier vendors.

What is keeping you from assessing all of your vendors, or all of your top-tier vendors?



How long, on average, does it take you or your team to complete a vendor assessment for your top-tier vendors?



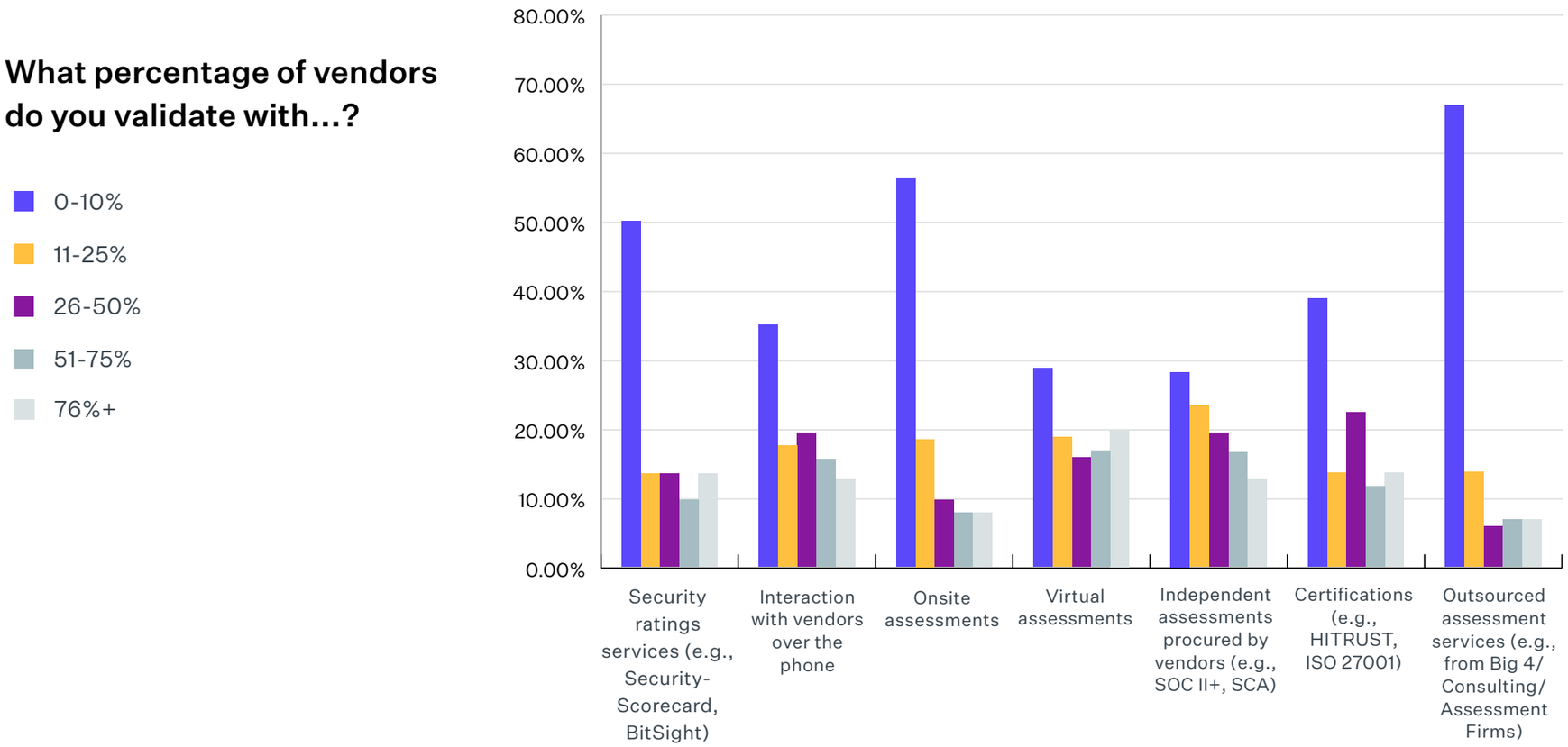
Speaking of Costs...

The predominant mechanism for validating the greatest number of vendors once assessments are complete was virtual assessments with 20% of respondents indicating so. This is to be expected, as this is a less expensive route than, say, onsite assessments.

The more "expensive" validation types are used most frequently to assess a fewer number of (presumably) high-priority vendors, likely due to the cost of doing so. For example:

- **67% of respondents assess fewer than 10% of their vendors using outsourced assessment services (e.g., from the Big 4 accounting firms).**
- **56% of respondents assess fewer than 10% of their vendors using onsite assessments.**
- **51% of respondents assess fewer than 10% of their vendors using security ratings services (e.g., SecurityScorecard, BitSight).**

What percentage of vendors do you validate with...?

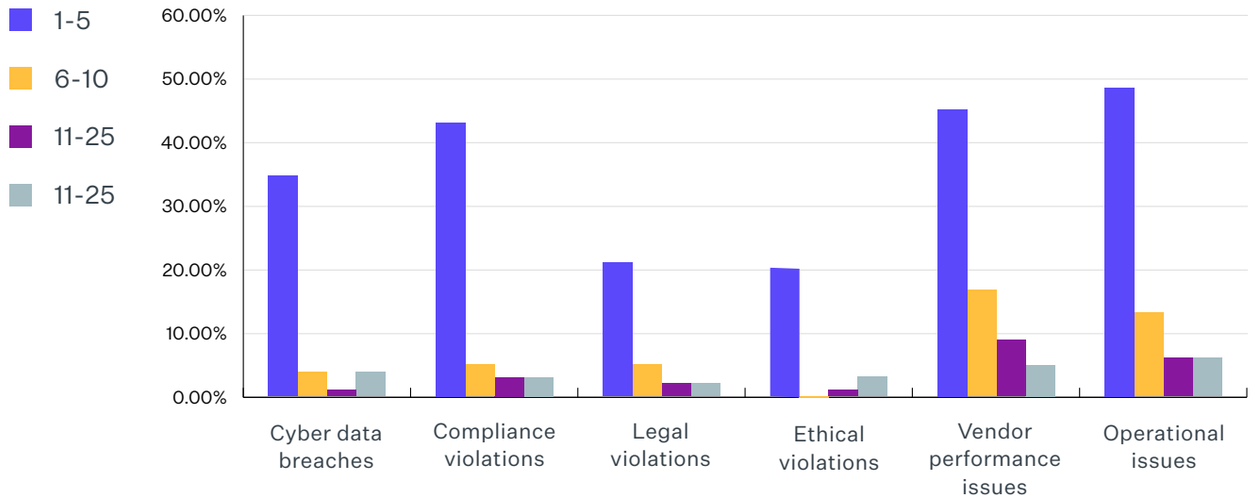


Consequences

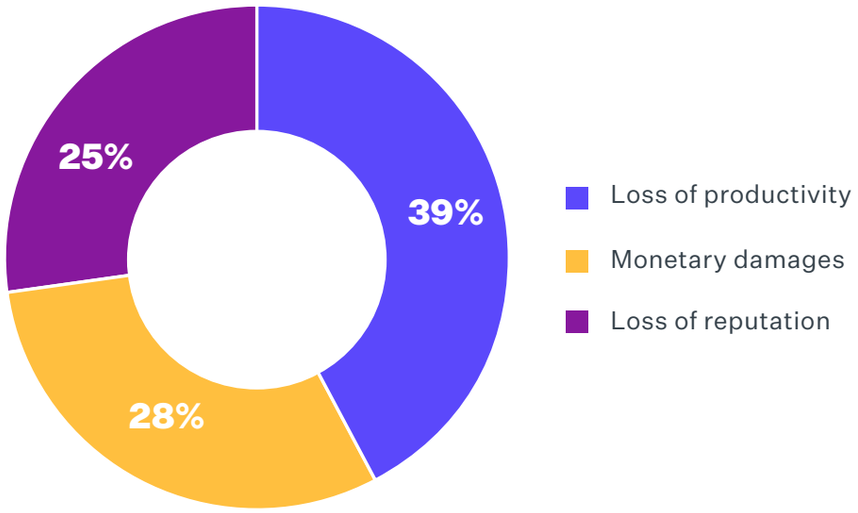
Finding #6:
There Are Real Consequences to Not Getting Third-Party Risk Right

When asked if any incidents were experienced within the past two years that originated with a third party, 76% of the respondents said that they experienced one or more issues that impacted vendor performance, followed by operational issues (74%), with 55% indicating a compliance violation.

How many incidents of the following types have you experienced within the past two years that have originated with a third party?



Third party incidents resulted primarily in:



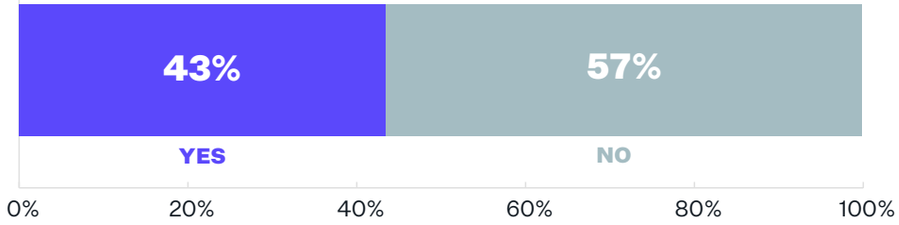
Frustrations

Finding #7:
Most Existing Toolsets Aren't Cutting it

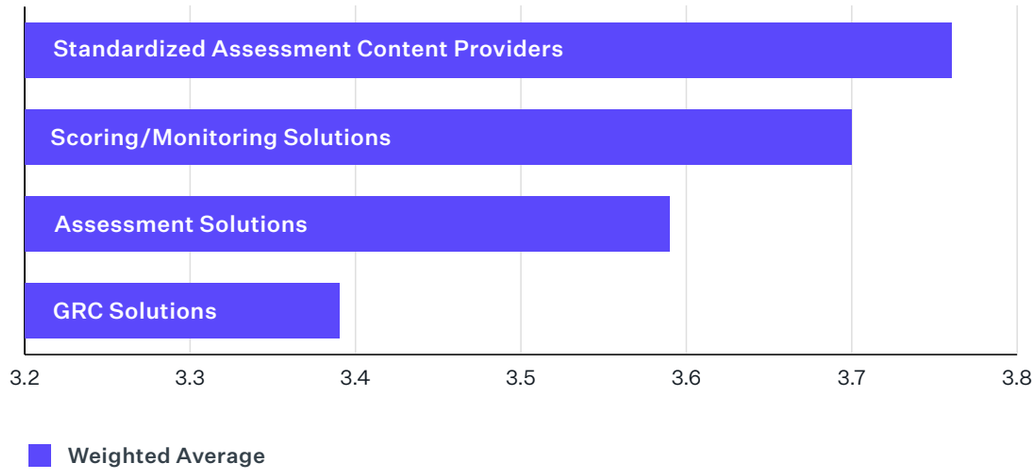
When asked if they were planning to implement a new or augment/replace an existing third-party risk management solution in the next 12 months, nearly half of respondents said yes. When half the market is looking to change their solution, it must mean needs aren't being met.

And it's no wonder, considering that the satisfaction levels among existing tools hovers in the 50% range, and weighted average of satisfaction caps out at 3.8/5.0. GRC tools have an especially long way to go with a 41% satisfaction rate (RSA® Archer® and ServiceNow® were the two most frequently named). However, Standardized Assessment Content Providers buck this trend, delivering a weighted average satisfaction of nearly 3.8/5.0 – organizations are evidently relying on standardized assessment content to help clear the path.

Are you planning to implement a new, or augment/replace an existing, third-party risk management solution within the next 12 months?



What is your level of satisfaction with each of the solutions you mentioned in the previous responses?



Initiatives

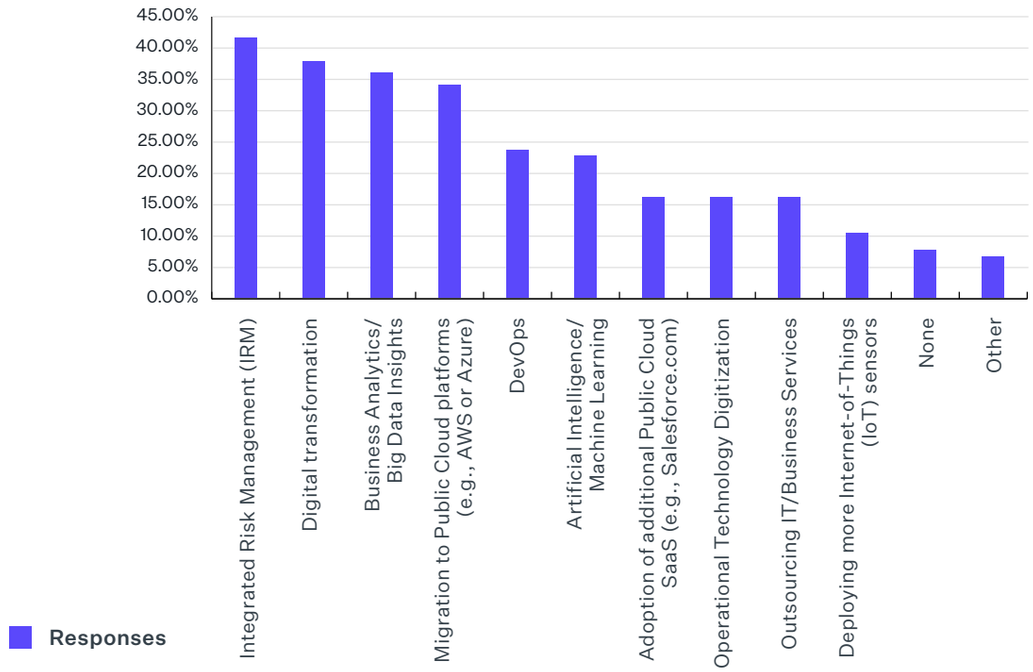
Finding #8:

IRM is a Top Initiative in 2020, but Resourcing, Change Management and Integration are Blockers

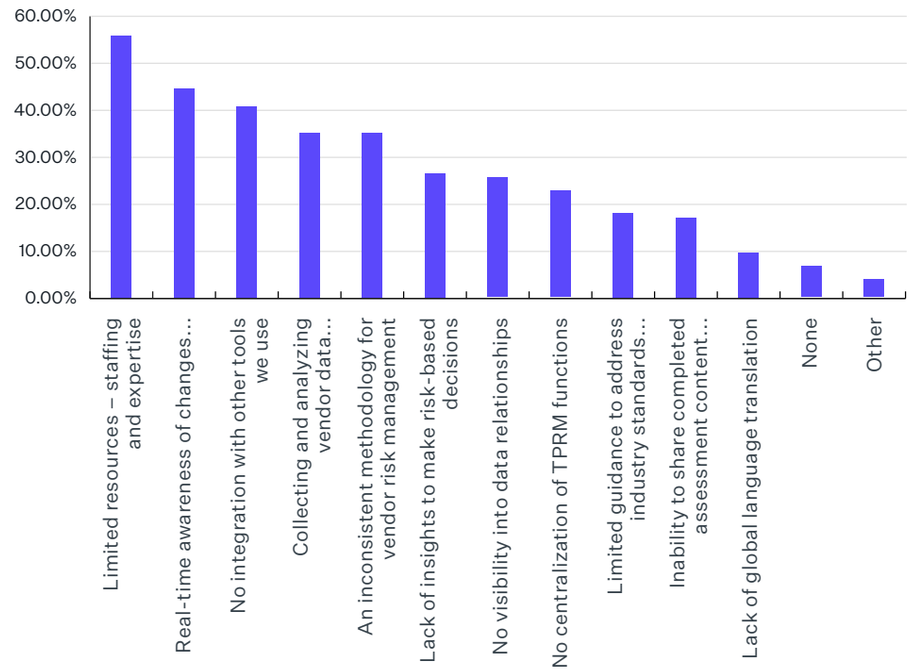
To address their regulatory and cyber challenges, respondents indicated that top projects for their organizations in 2020 included integrated risk management (42%), digital transformation (38%), and business analytics/big data insights (36%) but they see challenges ahead in achieving these business goals. Limited resources/staffing/expertise (56%), no real-time awareness of changes (44%), and no integration with other tools used for vendor management or risk management (41%) are seen as the biggest inhibitors to deploying transformative new technologies.

IRM might be the top initiative for 2020, but clearly organizations are concerned they won't get the resources required to manage it; that it won't deliver the real-time insights to help make changes; and that it won't have the integrations into other business systems to simplify risk management.

What are your top business projects for 2020?



What are the third-party risk management-related roadblocks to moving forward with these business projects?

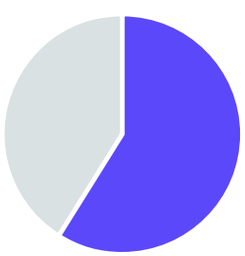


Initiatives

Finding #9:
What Practitioners Are Looking For

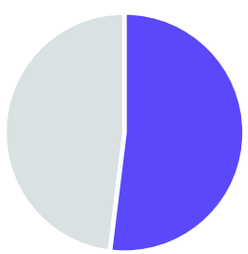
When asked what capabilities they wanted to help address their challenges, respondents indicated that the most important capabilities were reporting on the most critical relevant risks (59%), a vendor inventory (52%), and a repository of completed assessments (51%).

These asks are clearly aligned with the challenges organizations face in terms of resources, costs and lack of real-time visibility.



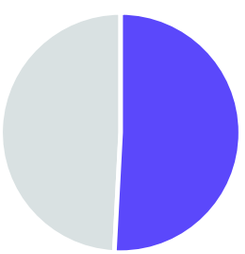
59%

want reporting on the most critical relevant risks



52%

want a vendor inventory



51%

want a repository of completed assessments

Recommendations

Growing and maturing an adaptable and agile third-party risk management program doesn't have to be a complex and time-consuming process.

Here are some recommendations to jump start your vendor risk activities:

Develop a Programmatic Process

The results of this study clearly showed that organizational third-party risk maturity levels are all over the place – but risk management teams must accelerate their program maturity levels to stay ahead of vendor performance, operational and compliance problems.

A programmatic process should help your team progressively:

- Define who your vendors are and what inherent risks they present to your business
- Assess the right strategy to collect the right insights from the right third parties
- Analyze results from assessments and score risk levels based on a broad ecosystem of inputs
- Remediate risks raised from analysis of completed assessments
- Report against industry and regulatory requirements, and for the board
- Optimize the program to adapt to changing requirements and resource levels

The outcomes of such a standardized and repeatable methodology will be:

- A roadmap to program maturity with defined milestones, goals and outcomes
- Onboarded vendors that are tiered, categorized and have an inherent risk score
- The right questionnaire for your team's needs
- A collection method that enables flexibility and scale
- Analytics-based decision making
- Continuous monitoring of your program based on success criteria

Recommendations

Build a Cross-Functional Team

TPRM requires collaboration between internal teams that have their own specific expertise, like Cybersecurity, Legal/Compliance, Procurement, and others. TPRM can thrive by leveraging external partners that can bring missing expertise from the outside. Optimizing the process for identifying issues and measuring risk is essential, but organizations also need to know how to fix the problems once the assessment process is done. Given the complexity, no one person can likely figure all that out, so internal and external collaboration is key to not just identifying risk but mitigating it, too.

Be Comprehensive Without Being Complex

A comprehensive set of questionnaires enables flexibility in assessing vendors. For example, consider the regulatory priorities this study revealed: GDPR, SOC 2, ISO, PCI and NIST. Maintaining multiple unique question sets for each can tax already time-constrained teams.

There are solutions available on the market that offer a library of pre-defined questions that map back to any number of regulatory or industry frameworks. This lets you avoid the duplication of effort and patchwork of requirements you would get if you tried to individually assess each framework. It's also much easier to prove compliance when it's one question that covers many requirements at once.

The other benefit of using standardized content like this is that there's a good chance that the organization you're assessing will have already seen the questions phrased this way. You may not have to wait weeks for them to fill out your questionnaire, and you will both already be speaking the same language when it comes time to figure out what to do about any problems you find.

Recommendations

Stay Agile with Options for Assessment and Analysis

Don't pigeon-hole yourself into a single rigid option for collecting and analyzing surveys from your third parties. There are multiple ways to assess all of your top-tier vendors (and thereby overcome a major challenge cited in this survey).

- **Self-service:** Collect just the basics to inform your profiling and tiering logic, or fully assess vendors yourself. At the very least, centralize the management of all your vendors into a single place so you maintain visibility.
- **Managed service:** Outsource the assessment of your top-tier third parties to a specialist in risk identification and analysis, and free your team to focus on long-term, residual risk management.
- **Shared service:** Leverage a network of completed vendor questionnaires and supporting evidence for your lower-tier vendors, so you can focus your team's efforts (and the correct amount of resources) on higher-tier vendors.

Complement Your Decision-Making with Risk-Based Intelligence

Making decisions in silos with a limited dataset will not enable your team to be effective vendor risk managers. Instead, seek out solutions that are built on an open platform with integrations to multiple business and risk solutions. A solid solution will offer:

- A comprehensive risk profile that informs assessment tiering, assessment frequency, and SLA measurement
- A quantified and contextualized risk model inclusive of cyber risks and business risks, plus ISO and FAIR calculations
- Response management with enabled workflow and automation to ensure that vendor intelligence is routed to the right people on your team
- Risk reporting and prioritization, including context and guidance for prioritization
- Automated dissemination of reports to ensure transparency with third parties and within your organization

Conclusion

Like a third rail, third parties can help power your enterprise, but they can also pose a significant risk if not handled correctly.

Existing tools and IRM solutions aren't enough to overcome third-party risk management challenges. Only a comprehensive model that offers a programmatic process to maturity, with options to manage costs and compliance reporting, will provide a solid foundation for risk management teams to adapt over time.

For more on how Prevalent can help address your third-party risk management challenges, visit www.prevalent.net. You can also download the infographic here.

Shared Assessments provides best practices, solutions and tools for third-party risk management. Learn more at www.sharedassessments.org.

Note: Demographics of the 2020 Third-Party Risk Management Study
The typical respondent to the 2020 Third-Party Risk Management Study was a US-based manager in security or IT with complete or quite a bit of involvement in third-party risk; in a highly-regulated company of about 2,350 employees (median) or 27,000 employees (mean); and doing business primarily across the US, Canada, the UK and the EU.