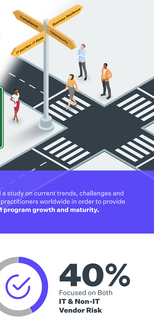
Prevalent

The 2022 Third-Party Risk Management Industry Study



TPRM Programs Are at a Crossroads

In February and March 2022, Prevalent conducted a study on current trends, challenges and initiatives impacting third-party risk management practitioners worldwide in order to provide **actionable recommendations for TPRM program growth and maturity.**

Broadening Risk Drivers

40% Focused on Both **IT & Non-IT Vendor Risk**

45% of TPRM Programs Are Mostly Focused on **IT Vendor Risk**

It should come as no surprise that the main focus for TPRM programs is IT vendor security risk, as cited by 45% of respondents.

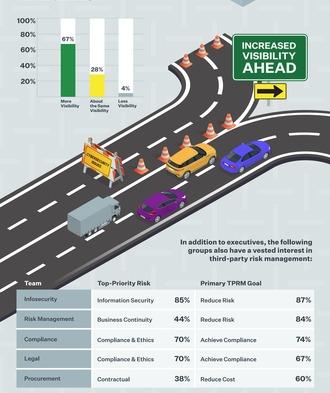
However, a surprising **40% of respondents** in 2022 say they **are focused on managing both IT and non-IT vendor risks.** This is a positive trend.

Why? Supply Chain Disruptions and Compliance Violations Are on the Rise

In 2022, 55% of respondents said they experienced an audit finding related to a third party and 54% said they experienced a supply chain disruption. 45% of respondents report their organization has experienced a data breach or other security incident connected to a third party in the last 12 months. All numbers are up dramatically from 2021, signaling the need to track IT security and non-IT security risks alike.

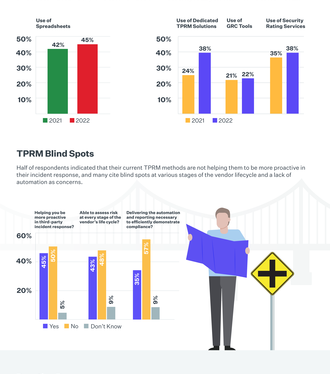
Third-Party Issues in the Last 12 Months:

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



Increasing Organizational Awareness

More than two thirds of respondents indicated that their third-party risk management program has more visibility among executives and the board compared to last year.



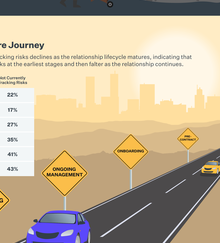
In addition to executives, the following groups also have a vested interest in third-party risk management:

Team	Top-Priority Risk		Primary TPRM Goal	
Infosecurity	Information Security	85%	Reduce Risk	87%
Risk Management	Business Continuity	44%	Reduce Risk	84%
Compliance	Compliance & Ethics	70%	Achieve Compliance	74%
Legal	Compliance & Ethics	70%	Achieve Compliance	67%
Procurement	Contractual	38%	Reduce Cost	60%

The State of TPRM in 2022

A disappointing 45% of respondents indicate that they are **still using spreadsheets** to assess their third parties in 2022 – a slight increase from 2021.

It's not all doom and gloom, however. Reported use of **dedicated TPRM solutions**, **GRC tools** and **security rating services** has increased in 2022.



TPRM Blind Spots

Half of respondents indicated that their current TPRM methods are not helping them to be more proactive in their incident response, and many cite blind spots at various stages of the vendor lifecycle and a lack of automation as concerns.

Reactive Response

A concerning number of respondents don't have any third-party incident response program in place (8%) or take a passive approach to incident response (23%).

8% Have **NO third-party incident response** program.

23% Learn about security incidents **from their third party or a news article.**

69% **Reach out to third parties after an incident** to determine their exposure.

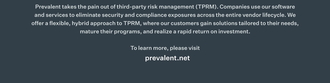
In all, it takes about 2.5 weeks from when an organization learns of an incident to when they receive confirmation of remediation.

Benchmarks and Reporting Time

TPRM practices are prominently featured in several security, privacy, and ESG regulations – as well as in NIST, ISO, SOC 2 and other frameworks – so compliance continues to be a burden for respondents.

Time it takes organizations 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%



Not Tracking the Entire Journey

The percentage of respondents tracking risks declines as the relationship lifecycle matures, indicating that companies are focused more on risks at the earliest stages and then falter as the relationship continues.

	Not Currently Tracking Risks
Sourcing & Pre-Contract Due Diligence	22%
Onboarding	17%
Assessing & Monitoring	27%
Ongoing Management	35%
Contractual Performance	41%
Offboarding & Termination	43%

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.

Expand Assessments Beyond IT Security Under a Single Solution

Looking at third-party risk solely through an IT lens will miss important risks. Invest in a solution that goes beyond rich questionnaire templates and intelligence to address a broad range of risks to improve reporting, eliminate spreadsheets and accelerate audit reviews.

Automate Incident Response to Reduce Cost and Time

Third-party incidents are on the rise and can take more than two weeks to resolve. Invest in automation and a solution that centrally manage all vendors, identify which ones are at risk, provide early warning of incidents, quickly mitigate risks and satisfy regulators.

Close the Loop on the Third-Party Lifecycle

Issues can crop up at any time during a vendor or supplier relationship. Choose a TPRM solution that supports contract lifecycle management capabilities and conduct a final risk assessment during offboarding to validate that your systems and data are securely decommissioned in compliance with data privacy mandates.

Download the Study >

Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate security and compliance exposures across the entire vendor lifecycle. We offer a flexible, hybrid approach to TPRM, where our customers gain solutions tailored to their needs, mature their programs, and realize a rapid return on investment.

To learn more, please visit
prevalent.net