Prevalent.

Third-Party Risk Program Maturity: Don't Let It Slide

Organizations **face a slippery slope** when they unknowingly allow vendors to expose them to cyberattacks and other threats to security, privacy and compliance. Climbing the third-party risk management (TPRM) ladder to full program maturity is the only way to fully ensure business and supply chain resilience.

Prevalent conducted a thorough TPRM Program Maturity Assessment of dozens of organizations and found several critical areas where a majority of companies are at risk.

Request a TPRM Maturity Assessment

Overall Maturity Average | 2.53

We measured program maturity in five key areas: Coverage, Content, Roles and Responsibilities, Remediation and Governance. On a scale of one to five, where five represents full program maturity, respondents averaged an **alarming overall maturity score of just 2.53.**

Critical Risk Area:

Content

Risk: Not Creating a Centralized Risk Register

Lacking a clear and standardized third-party risk register to present findings makes the review process difficult to manage and risk trends hard to identify.

52% **didn't have a standard way to present risk data**

Recommendations:

- **Review vendor questions** and response options to ensure consistency with scoring logic
- **Calculate a risk score** on a per question basis to prioritize the data
- **Create an itemized list** of unsatisfactory responses to follow up on

Critical Risk Area:

Roles and Responsibilities

Risk: Lacking a Standardized Process

Without an operational manual to guide the assessment workflow, processes may not be standardized and managing personnel changes can be a challenge.

62% **lacked a standardized TPRM process**

Recommendations:

- **Conduct a workshop** to identify the key operational workflows and associated owners
- **Document processes**, accountability, supporting roles and responsibilities

Risk: Failing to Examine Resource Requirements

If resource requirements are not weighed against the volume of third parties and extent of the review process, then a resource shortage could prevent the program from meeting its objectives.

52% **had resource planning shortfalls**

Recommendations:

- **Review and forecast** resource requirements for your TPRM program
- **Do this well in advance** of any changes to program scope
- **Estimate time for task completion** to calculate the maximum capacity of the program

Risk: Using Expensive Resources for Simple Tasks

Information security subject matter experts are often needlessly burdened by the operational aspects of assessments, such as issuing questionnaires, checking completeness, and resolving issues.

59% **overspent on TPRM resources**

Recommendations:

- **Map program processes** to skill set requirements
- **Align representatives** to tasks based on expertise
- **Avoid using subject matter experts** for administrative tasks

Critical Risk Area:

Coverage

Risk: Stopping at Third Parties

Assessment processes often don't consider fourth parties (i.e., "third parties of your third parties") that are critical to services and can pose unidentified risks and operational bottlenecks.

79% **didn't consider fourth-party risk**

Recommendations:

- **Incorporate key fourth parties** into your third-party assessment process
- **Identify where fourth parties could have an effect** on the confidentiality, availability of services, financials, reputation, data privacy and more

Critical Risk Area:

Remediation

Risk: Not Standardizing Remediation Guidelines

Without standardized guidelines, the process of reviewing risk findings with third parties can be inconsistent , leading to misalignment with organizational requirements.

86% **had inconsistent remediation guidelines**

Recommendations:

- **Identify the minimum criteria** to justify a status change for each question
- **Determine what evidence** is needed to support these decisions
- **Standardize what your organization** is willing to accept and what must be remediated

Risk: Not Scoring Risk Likelihood and Impact

Identifying and prioritizing findings can be resource intensive and inconsistent without a scoring mechanism to weight the impact and likelihood of risks based on responses.

59% **had incomplete risk scoring mechanisms**

Recommendations:

- **Review and understand** what risk each question is trying to identify
- **Weight the questions** based on risk likelihood and impact on the organization

Critical Risk Area:

Governance

Risk: Limiting Risk Reporting to Tactical Uses

Until risk reporting is used to drive strategic internal conversations, it is difficult to make informed decisions about emerging threats, areas of concern, change assessment and risk remediation.

69% **were missing strategic reporting opportunities**

Recommendations:

- **Aggregate risk data** across the program scope
- **Use identified items** to assist the third-party program and cyber security initiatives
- **Identify noteworthy observations** and key events for consideration in strategy sessions

Risk: Lacking a High-Level Understanding of Third-Party Risk

Without a method of providing sufficient reporting across all third parties, you may not have a full and accurate picture of program findings and key areas of organizational risk.

59% **struggled to gain an overall view of third-party risk**

Recommendations:

- **Perform an exercise to aggregate** third-party assessment data
- **Give special consideration** to non-responsive third parties, risk trends and forecasted scoring
- **Use the aggregated data** to steer decision making and strategy

Know Where You Stand

If you're unsure where your organization is on the TPRM ladder, sign up for a free Maturity Assessment consulting session. You'll walk away with an in-depth report on the state of your current program, plus practical recommendations for how to bring it to the next level.

Request a TPRM Maturity Assessment

Pressed for time? Answer 10 multiple-choice questions to get an instant "gut check" of your third-party risk readiness.

Get Your Free Risk Score

Prevalent.

Existing toolsets and integrated risk management solutions are not enough to overcome today's top vendor risk challenges. Prevalent is the only company with a comprehensive, 360° third-party risk management solution.

prevalent.net