ProcessUnity

The Third-Party Risk Crisis: How to Close Your Vulnerability Gap

Third-party risk is escalating. The number of third parties organizations rely on is surging, yet risk teams don't have available resources to manage the growing exposure. With manual processes and outdated models, companies face delayed risk responses, compliance failures, and costly security breaches.

The result? A widening third-party risk vulnerability gap that leaves organizations exposed.

The Data Tells the Story

The numbers paint a clear picture — third-party risk management is falling behind. Despite increasing awareness at the executive level, most organizations still struggle with outdated processes and incomplete risk assessments.

Growing Risk Exposure	Lack of Readiness	Leadership Awareness vs. Action

54% of breaches originate from third parties.

47% of organizations elevate TPRM to the board level — but gaps still persist.

Only **30%** of organizations assess at least half of their third-party relationships.

69% of risk leaders say their TPRM programs are still manual.

77% of executives say their TPRM program needs an overhaul.

Every company has a TPRM vulnerability gap — the question is, what unique circumstances determine the size of the gap for each business.

What Drives the Gap?

So, what's causing your vulnerability gap? A combination of seemingly uncontrollable pain points leaves organizations exposed to unnecessary risks. The most common challenges include:

Process Inefficiencies

- **Slow onboarding cycles** delay new services for business users.
- **Due diligence backlog** leaves vendors unchecked.

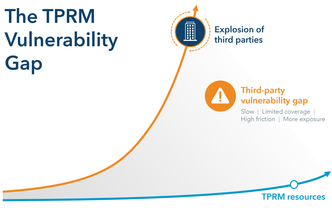
Limited Risk Visibility

- **Hard-to-assess vendors** create gaps in risk visibility.
- **Inadequate portfolio coverage** leaves unknown risks unaddressed.

Response Delays

- **Delayed threat response** exposes organizations to emerging risks.
- **Lack of vendor tiering** makes risk prioritization difficult.

The TPRM Vulnerability Gap



What Makes Up Your Gap?

- Lack of a Standard TPRM Process
- Lack of Vendor Prioritization (Inherent Risk)
- Onboarding Cycle Times
- Hard-to-Assess Vendors
- Assessment Backlog
- Policy / Evidence Reviews
- Threat & Vulnerability Response
- Inadequate Portfolio Coverage

Closing the Gap

Organizations can no longer afford to operate with outdated TPRM models. The risks are too high, their business relies on too many third parties, and the costs of inaction continue to rise. To bridge the third-party vulnerability gap, organizations need a force multiplier — a modernized strategy that turns limited resources into a high-impact, scalable TPRM program.

The solution lies in four key components:

TPRM Automation:

Streamline assessments, onboarding, and monitoring to speed up processes.

Universal Data Core:

Centralize third-party risk data for a unified, real-time view of vulnerabilities.

Assessment Exchange:

Leverage pre-validated vendor assessments to accelerate due diligence.

AI-Powered Teams:

Use AI to enhance risk detection, review policies, and complete assessments.

Discover a Painless Approach to TPRM

Today's dynamic risk environment demands a more robust approach to third-party risk management. Organizations must move toward automation-driven, AI-enhanced, and data-integrated risk management strategies to effectively close their vulnerability gap. By adopting a modern, scalable approach, businesses can build a more resilient and proactive third-party risk management framework.

Download our whitepaper, **A Modern Approach to Third-Party Risk Assessments** to start closing the gap today!

Download Here

About ProcessUnity

ProcessUnity is The Third-Party Risk Management (TPRM) Company. Our software platforms and data services protect customers from cybersecurity threats, breaches, and outages that originate from their ever-growing ecosystem of business partners. By combining the world's largest third-party risk data exchange, the leading TPRM workflow platform, and powerful artificial intelligence, ProcessUnity extends third-party risk, procurement, and cybersecurity teams so they can cover their entire vendor portfolio. With ProcessUnity, organizations of all sizes reduce assessment work while improving quality, securing intellectual property and customer data so business operations continue to operate uninterrupted.

To learn more or request a demo, visit www.processunity.com.