Redefining Third-Party Risk: Transitioning to a Modern Risk-Based Approach with SAFE TPRM

CISOs Demand a TPRM Revolution

In today's interconnected business landscape, third-party relationships are both a boon and a bane. While they drive innovation and growth, they also open doors to potential cyber threats. The harsh reality is that 45% organizations have experienced third party-related business interruptions during the past two years, and this number shows a 68% year-over-year growth. This stark statistic underscores a critical gap in traditional third-party risk management (TPRM) methods, which are increasingly seen as inadequate in the face of sophisticated cyber attacks.

45%

Organizations have experienced third party-related business interruptions during the past two years

UnitedHealthcare okta SOLARWINDS

With cyber attackers continually targeting the most vulnerable points in the supply chain — often smaller, less protected vendors — the call for a TPRM revolution grows louder. Chief Information Security Officers (CISOs) unanimously agree that the conventional ways of managing third-party risks are failing: Traditional tools like self-assessment questionnaires and cybersecurity ratings are simply not cutting it. They do not measure or mitigate risks effectively, leading to wasted investments and heightened vulnerabilities.

...It's clear that innovative approaches to TPRM are not just necessary—they are essential for real security improvements.

The Resulting Frustration Among Leaders

The reliance on multiple tools without sufficient integration or a holistic view leads to several issues that frustrate TPRM stakeholders.

"I don't know where my critical risks are! It is a blind spot"

- CISO of a Fortune 100 healthcare provider

"I don't know what actions to take to reduce the risk"

- CISO of a Fortune 500 technology company

"My third-party program is non-existent or highly immature/ unscalable."

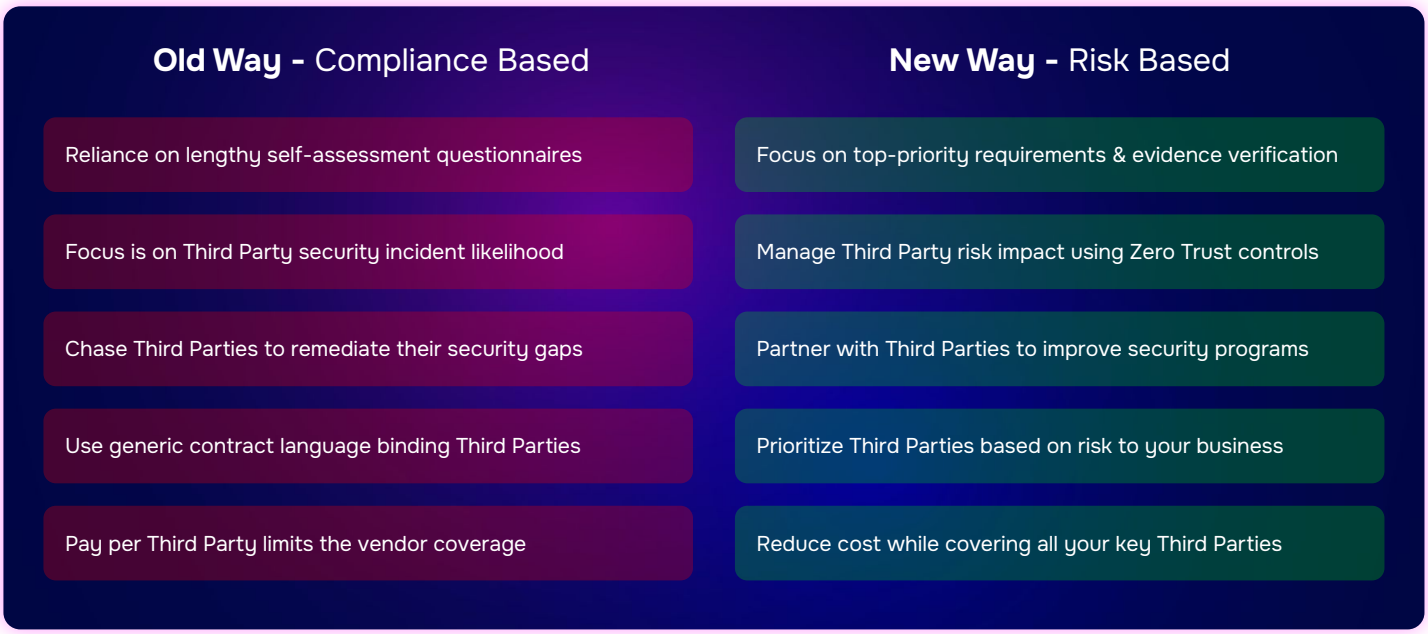
- CISO of a mid-market insurance provider

"I need a more automated process to prevent my team from burning out"

- CISO of a Fortune 100 manufacturing company

"I don't want to keep following up with my vendors to check their actions"

- CISO of a mid-sized retail company



Old Way: Compliance-Based Approach

- **Self-Assessment Questionnaires:** Traditionally, companies sent out detailed questionnaires to their third-party vendors, asking them to check off a long list of security measures/controls they claimed to have in place. The aim was to get a declaration of security readiness from these vendors, but this often just resulted in lists that might not reflect the real situation.
- **Focus on Incident Likelihood:** The goal was to lessen the chances of security issues by identifying security gaps through the questionnaires and pushing for them to be fixed. However, this approach was more about planning than practical action.
- **Chasing Remediation:** After identifying security gaps, companies often had to repeatedly follow up with third parties to fix these issues. Unfortunately, these efforts to get gaps remedied were frequently ignored or delayed, leaving unresolved security risks.
- **Generic Contract Language:** Contracts used broad, standard language that required third parties to comply with specific regulations and standards. While this sounds good on paper, it didn't ensure that third parties actually implemented solid, ongoing security practices.
- **Per-Party Payment Model:** This pricing model limited the ability to monitor and assess risks across all third parties effectively. It often meant only a select group of vendors were regularly checked, missing potential risks from others not covered due to budget constraints.

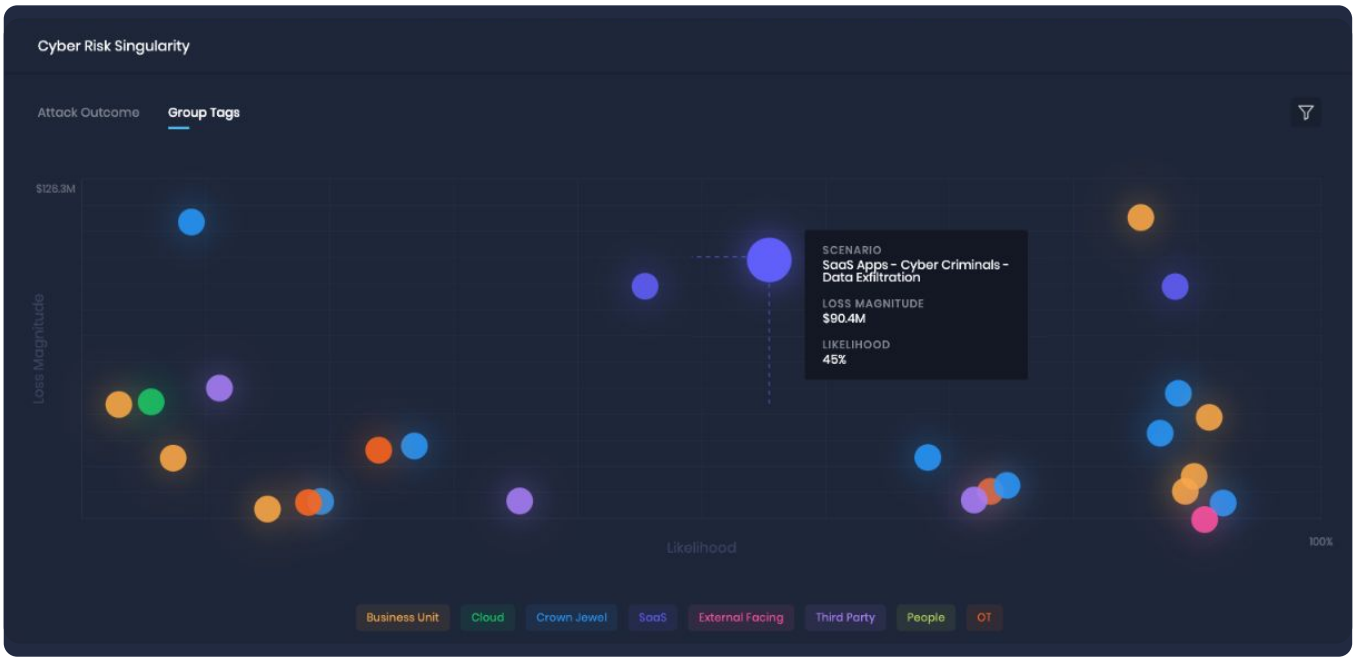
New Way: Risk-Based with SAFE

Focus on top-priority requirements and verify the evidence

SAFE TPRM simplifies third-party risk management by focusing on the most critical controls, derived from extensive research of current and past third-party cyber attacks. This eliminates duplication of effort and the need for third parties to respond to hundreds of questions, shifting the focus from quantity to quality of control assessments. By consolidating data from outside-in scans, questionnaires, and inside-out assessments, SAFE TPRM effectively assesses all controls and creates a laser focused prioritized list of critical controls.

Manage Third-Party Risk Impact Using Zero Trust Controls

SAFE TPRM promotes using zero-trust principles to handle third-party interactions safely. By assuming that all third parties could be potentially compromised, it urges enterprises to prioritize strengthening their internal defenses. This approach is akin to securing one's own house in a rough neighborhood before acting on the broader area. Implementing strict resilience controls within your operations minimizes the risks to your business.



Partner with Third Parties to Improve their Security Programs

SAFE TPRM makes it simple, swift, and efficient to collaborate with your supply chain using AI-assisted training and onboarding modules. These modules provide 24x7 support to vendors who have a direct SAFE One platform access. They can leverage the platform to visualize their cyber risk exposure and effectively prioritize their critical controls to reduce risk. This unique partnership enables third parties to manage cyber risk more effectively with security profile visualization, self-assessments, and training materials, and shrinks your third-party risk assessment cycle from weeks to days,

Prioritize Third Parties based on Risk to Your Business

SAFE TPRM assesses the dollar risk and likelihood of occurrence of the most frequent cyber risk scenarios such as ransomware, data breach attacks, and more based on third-party data access, network access, and resultant business interruption. This enables CISOs to tier their most critical vendors based on loss exposure instead of values such as size or revenue. SAFE TPRM enables enterprises to prioritize the most impactful controls to mitigate and reduce third-party risk.

Reduce cost while covering all your key third parties

SAFE TRPM acknowledges the dynamic nature of vendor risk management and its associated costs. Users of the platform can add an unlimited number of vendors at a fixed price since SAFE TPRM pricing is independent of the number of vendors – ensuring 100% of vendors are assessed. This scalable pricing model makes it practical to manage expenses of your growing third-party portfolio as the business expands.