COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2024

Wes Loeffler (wloeffler@fusionrm.com) is the Director of Third-Party Risk Management at Fusion Risk Management in Overland Park, Kansas, USA.

Navigating through uncertainty: The imperative role of third-party risk management

By Wes Loeffler

To compete in today's ever-changing business landscape and global economy, organizations are increasingly relying on their relationships with third to nth parties. The benefits include cost efficiencies, access to specialized services, and extended marketing reach. However, the costs of these relationships are often more difficult to gauge, extending beyond upfront business costs to the risks that may lie hidden within the third party.

This interconnectedness exposes organizations to a multitude of dangers—from financial and operational risks to cyber threats, regulatory fines, and reputational damage. Think of a line of dominoes: the longer the line, the more dominoes are likely to fall. Similarly, a geopolitical event in one region can lead to supply chain bottlenecks that not only affect direct suppliers but also have a ripple effect on secondary suppliers, logistics providers, and, ultimately, customers—hence the need for a robust and integrated third-party risk management (TPRM) program.

A multifaceted defense mechanism, TPRM is a series of checks and balances that provides a detailed picture of the potential pitfalls within an organization's supply chain and service providers. Having a proactive, strategic approach to TPRM allows organizations to not just mitigate risks but also turn risk management into a competitive advantage. By identifying and managing potential risks ahead of time, organizations can ensure they are not just protecting against potential losses but also positioning themselves to navigate the global landscape more nimbly than their competitors.

In essence, TPRM is a key element of business continuity and operational resilience in the modern era. The ability to predict, prepare for, and pivot in response to third-party risks can define the success or failure of critical operations. It's no longer just about managing risk; it is about managing your organization's future.

Why is integrated risk management a strategic imperative?

Today, visibility into third-party relationships is essential—not optional. Recent years have seen a global pandemic, geopolitical conflict in Eastern Europe, third-party cybersecurity vulnerabilities like Log4J, and other disruptions. Integrated risk management allows organizations to develop a holistic view of their operations that ties TPRM to broader strategies for business continuity and operational resilience. Managing third-party risk shouldn't be a siloed activity; it should be a strategic function about reinforcing continuity and resiliency at every level. An integrated approach brings a multidimensional benefit. It is about achieving a comprehensive understanding of risk across your extended enterprise and ensuring that every piece of the puzzle is positioned to support your overall resilience posture.

This can be achieved by establishing clear communication channels, fostering a risk-aware culture, and implementing technological solutions that enable the aggregation and sharing of risk information across the organization. To effectively build an integrated approach, organizations should align their risk management processes with strategic objectives, prioritize risks based on their potential impact, regularly communicate risk-related information to stakeholders, and continuously monitor and evaluate the effectiveness of their risk mitigation efforts. It is also important to provide adequate training and resources to employees involved in risk management to ensure their capability to address risks in a coordinated and integrated manner.

How do proactive risk assessments fit?

Reactive risk management is no longer sufficient; it's like trying to fix an already-sinking boat. Proactive risk assessment is about staying ahead. Organizations should focus on continuous monitoring, scenario planning, and stress testing against disruptions such as geopolitical shifts. This equips organizations to anticipate and prepare for disruptions rather than being caught off-guard. Anticipation is vital in managing third-party risk—it's the difference between proactive or reactive. Organizations must be able to foresee and plan for potential disruptions, changing the business dynamics from chasing to leading.

Continuous monitoring, in particular, is a essential component of an effective TPRM program. An effective continuous monitoring solution should start by identifying the key risk indicators that need to be monitored. These may include vendor performance metrics, security vulnerabilities, and compliance status. Next, select a suitable continuous monitoring tool or platform that can integrate with existing systems and provide real-time insights. Configure the tool to collect and analyze relevant data points, set up alerts and notifications for any potential risks or anomalies, and establish regular reporting and review processes. Finally, ensure proper governance and collaboration between the risk management team, the IT department, and vendors to effectively leverage the continuous monitoring solution for proactive risk mitigation.

How do strategic frameworks protect against third-party vulnerabilities?

It's imperative to develop strategic frameworks with a deep understanding of the potential risks that third-party operations might harbor. This is about more than just setting up defenses; it's about maintaining continuity and resiliency. Leverage technology and collaborative partnerships to ensure your frameworks are robust and can evolve with the threat landscape. Work closely with and monitor third parties to ensure they meet resilience standards. This is especially true where regular audits and due diligence become routine in the risk management and TPRM lifecycles.

To effectively implement strategic frameworks into your TPRM program, start by selecting a suitable framework that aligns with your organization's goals, industry standards, and regulatory requirements. Commonly used frameworks include the Standardized Information Gathering (SIG) questionnaire, International Organization for Standardization (ISO) 27001, and National Institute of Standards and Technology (NIST) SP 800-53. Once selected, thoroughly analyze and understand the framework's requirements and guidelines. Develop a roadmap for incorporating the framework into your risk management program, including the necessary policies, processes, and controls. Train your risk management team and relevant stakeholders on the framework and its implementation. Regularly monitor and assess compliance with the framework and adjust as needed to ensure ongoing alignment with best practices and emerging risks.

How do adaptive solutions help respond to real-time changes?

The real test of a risk management strategy is its adaptability. Organizations need real-time data, dynamic and agile management protocols, and pivot-ready and innovative technology. For example, adopting artificial intelligence (AI) and machine learning for predictive analytics represents a transformative leap in anticipating

the risk landscape. These types of technologies extend the sight line into the future of potential disruptions, granting organizations the capability not only to foresee but also proactively adjust to the ever-changing dynamics of global operations. This type of agility ensures that responses are not just timely but also strategically informed, keeping your organization, customers, partners, and stakeholders secure amid the tides of change.

AI, in particular, can expedite TPRM assessments by automating and streamlining various tasks. AI algorithms can analyze vast amounts of data from different sources—including contracts, financial statements, and regulatory filings—to quickly assess third-party risks. This automation enables faster identification of potential risks, helps prioritize assessments based on risk levels, and allows risk professionals to focus on higher-value activities such as analysis and decision-making. AI-powered tools can also flag anomalies and patterns, helping to proactively detect emerging risks and expedite response times.

What does it all look like in practice?

Actionable, integrated risk management identifies risks but, more importantly, provides a clear, proactive path to mitigating them. It begins with executive buy-in and filters down to every level of process implementation and technology adoption. It's a systematic approach to risk identification, robust technology for monitoring, effective communication with third parties, and a continuous cycle of improvement to keep the strategy agile and responsive. An effective integrated risk management strategy is never static; it's a living, breathing process that continuously adapts and evolves. It's the synthesis of committed leadership, thorough analysis, cutting-edge tools, and an unwavering commitment to innovation and improvement.

Final reflections

The need for a robust TPRM strategy is evident in a fast-changing and disruptive world. The unique vantage point offered by an integrated approach to risk management, proactive risk assessments, strategic continuity and resilience frameworks, and real-time adaptive solutions is not just a competitive edge—it's a necessity for survival and success in times when crises are continuously compounding.

Organizations must now view TPRM not as a standalone task but as an integral part of their strategic operations, echoed by the C-suite and board throughout the entire organization. The resilience of an organization's operations and its capacity to maintain continuity largely depend on the strength of its TPRM strategy.

The stakes have risen far beyond mere compliance or periodic due diligence; they now command a central role in shaping an organization's resilience and agility. The sweeping scope of an integrated risk management approach encompasses proactive risk assessments, strategic continuity and resilience frameworks, and real-time adaptive solutions.

Organizations must consider the broader implications of third-party risk on their customers and stakeholders, brand image, and reputation. Negative incidents involving third parties can erode trust and customer confidence, leading to long-term damage. A robust TPRM strategy is necessary not only for protecting assets but also for safeguarding intangible assets like reputation and trust.

To achieve this, organizations need to foster a culture of risk awareness and accountability across all levels. Employees should be educated about the importance of vigilance in third-party interactions and have clear guidelines for reporting potential risks or breaches. A transparent and proactive approach to risk management will help organizations identify and address issues before they escalate into crises.

For modern organizations, the challenge is expanding their vision and deeply integrating TPRM into their

operational strategy. The future will belong to those with the foresight to anticipate risk and the agility to adapt to the rapidly changing tides of global enterprise. This will ensure that they can remain resilient in the face of the unexpected and pivot with precision when the moment demands.

Takeaways

- Integrated risk management is vital, as it enables organizations to understand the resilience of critical third parties that are supporting *their* most essential products or services, which, in turn, strengthens operational resilience initiatives and ensures a strategic and dynamic approach to business continuity.
- Proactive risk assessments that leverage tools like continuous monitoring and artificial intelligence (AI) are crucial, as they enable practitioners to focus more on anticipating and preparing for potential disruptions and shift from a traditional reactive approach to a more strategic, forward-thinking stance.
- Strategic frameworks are crucial for continuity and resiliency, along with combining technology, collaboration, and regular audits to evolve defenses against third-party risks and ensure continuity of fundamental operations.
- Adaptive solutions using AI and machine learning for predictive analytics are fundamental for real-time, informed responses to geopolitical changes and help ensure business continuity, operational resilience, and the security of operations and the extended enterprise.
- An actionable integrated risk management strategy combines leadership commitment, systematic risk analysis, cutting-edge technology, and continuous innovation and improvement to effectively mitigate and prepare for risks.