KPMG

The partner paradox:

How to thrive in an evolving risk landscape

Drive maximum value from complex partner ecosystems

kpmg.com

Introduction

Modern businesses depend on third-party providers to help create value, offset risk, and exploit opportunities. As businesses divest assets, move key components of their operations to managed services, and transition toward AI-centric operations, these intentional ecosystems show no signs of slowing down: 83 percent of executives surveyed by KPMG LLP say their organization plans to expand their network of partners over the next one to three years.[1]

of executives surveyed by KPMG LLP say their organizations plan to expand their network of partners over the next one to three years.

The most valuable partners offer products or services that the business at the center of the ecosystem can't or won't deliver itself. However, even the most sought-after third-party products and services can bring risk to ecosystems, especially in highly unpredictable or complex markets. And, although shared responsibility and coordinated response models help mitigate vulnerabilities, a single point of failure can quickly topple an entire partner network.

Regional conflicts, for example, serve as a reminder of the importance of alleviating concentration risk. Nearly one quarter of respondents to a World Economic Forum survey cite geopolitical tension as the most severe global risk for 2025,[2] given the potential for breakdowns in human relationships, trade routes, and resource availability. Fluctuating tariffs and evolving regulations also necessitate careful tracking as disruptions can bring operations to a halt. Even cloud-based technologies and AI, usually considered problem solvers instead of instigators, expand the attack surface and introduce new cyber and privacy threats.

As compound volatility turns the normal course of business on its head, companies—and their partners—must adopt proactive, end-to-end, intentional risk management. In this paper, we explore the interconnected risks associated with partner ecosystems and offer recommendations to create an integrated and precise third-party management strategy.

Rethinking the performance and risk management framework

The traditional approach to third-party risk management focuses on compliance and contractual obligations. Organizations typically conduct initial due diligence, assess financial stability, align on a cybersecurity posture, and review legal compliance, with periodic assessments to verify adherence.

These tasks, although foundational to third-party risk management, leave businesses unable to quickly tackle new threats or unexpected changes. By not accounting for complex interdependencies and broader risk factors, such as cybersecurity threats or geopolitical fluctuations, an unexpected threat can leave the businesses in an ecosystem flat-footed.

17% **of KPMG survey respondents have developed extended resiliency plans beyond critical processes.**

50% **of respondents to a recent KPMG risk management survey said they do not yet rank their vendors and third-party providers by risk level.**

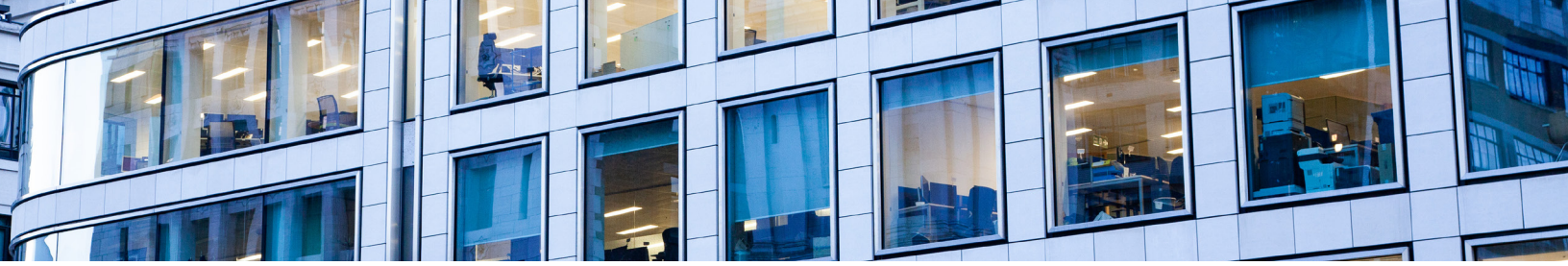
KPMG research discovered that most businesses are unprepared to find and face their blind spots: Only 17 percent of organizations we surveyed have extended resiliency plans beyond critical processes.[3] Further, only half of respondents to our recent Risk and Resiliency Survey say they have centralized or coordinated structures for managing risk and resiliency.[4] This matters because businesses that centralize risk and resiliency planning are more mature in their ability to respond to disruption, more likely to use specialized tools for the majority of risk processes, and twice as likely to have timely data.

Segment potential partners according to risk factors

The most resilient organizations methodically segment third parties within their ecosystems according to risk, considering various factors from compliance to financial stability to technology. However, at present, 50 percent of respondents to a recent KPMG risk management survey said they do not yet rank vendors and third-party providers by risk level.[5]

In the current environment, it is critical to evaluate potential partners' compliance risks, which encompass regulatory and statutory compliance, ethics, and conduct. Strategic risks, such as geopolitical factors, mergers and acquisitions, and the introduction of new products and services, should also be top of mind. In the realm of information security and technology risk, organizations need to evaluate whether partners could be introducing threats related to emerging tech, cybersecurity, privacy, and AI.

Operational risk is another significant concern. Organizations should assess model oversight, the concentration of dependencies, partners' involvement of subcontractors (including fourth and fifth parties), their operational resiliency, and the efficiency of performance and service delivery. Legal risk is also critical considering the potential for sanctions or threats of litigation involving partners—threats that could have an impact on the business at the center of the ecosystem by association. Fraud risk is another area that merits vigilance, with incidents of bribery and money laundering growing worldwide. Financial risk should be carefully examined, focusing on partners' financial viability, liquidity, and market credit. Lastly, reputational risk can be addressed by monitoring negative news and managing brand perception of both the organization and its partners.



Emerging risks to prioritize in your risk management strategy

Although regulatory changes are leading nearly one in three businesses to invest in compliance and risk management,[6] an array of uncertainties threaten enterprise stability. The divergence of US and European regulations, for example, is impacting information security and technology risk management expectations, compliance requirements, and operational risk responses.

Information security and technology risk

Most businesses surveyed by KPMG are prioritizing tech partnerships,[7] but connected technologies like AI, the Internet of Things, and blockchain also introduce new vulnerabilities. As highlighted in a recent letter from JP Morgan Chase to third-party suppliers,[8] the dependence on SaaS as the default format for software delivery is "embedding concentration risk into global critical infrastructure." In other words, if a breach or an outage occurs, the resulting single points of failure could have catastrophic consequences throughout the system.

By integrating protocols to manage these risks into their third-party risk mitigation frameworks, organizations can ensure they are aligned with partners on cybersecurity, data privacy, and ethical standards; specify how partner applications, software, and hardware should be implemented and managed; and agree on the division of responsibility should a breach or technology disruption occur. More important, by pursuing implementations of AI and other digital technologies with firm guardrails in place, organizations and their partners can innovate and move more quickly to market with new joint offerings.

Compliance risk

Deregulation in the US might offer a temporary break from onerous reporting requirements domestically, but American companies and partners that conduct business abroad will need to keep pace with international compliance rules. The sustainability regulatory landscape is particularly fragmented, even for domestic partnerships: Although federal climate disclosure rules have stalled in the US, state-level mandates are gaining momentum.

Since global data-sovereignty regulations are in flux, companies should establish mechanisms for managing the patchwork of regulations that may apply. When the company and its partners have varying data residencies (the physical locations where data are stored), further complications can arise. By carefully monitoring and tracking the relevant privacy and data sovereignty laws stemming from data residency, organizations can minimize risks associated with cross-border data transfers, including unauthorized access, data loss, and security breaches.

Concentration risk

As companies take on partners that support, interact with, or execute on behalf of their supply chains, they need to be wary of overdependence on certain regions where distribution disruption may be more likely. In fact, 73 percent of respondents to a National Association of Manufacturers Outlook Survey cited trade uncertainties, including tariffs, as their top business challenge, up from 56 percent and 37 percent in its previous two quarterly outlook surveys, respectively.[9]

With tariff fluctuations, organizations are rapidly reconsidering supply chains and considering third parties where there may not be a long-standing relationship. Further, when it comes to mitigating the impact of unrest or tariffs on any of your ecosystem partners, assessing the country of origin (CoO) for critical supplies is essential. Remember that where a good is manufactured or transformed is not necessarily the country of export. For example, if a partner acquires more than 20 percent of product components from the US, tariffs can be mitigated. However, with products that move through numerous nations, such as pharmaceutical or automative components, determining CoO can be challenging.

Key recommendations

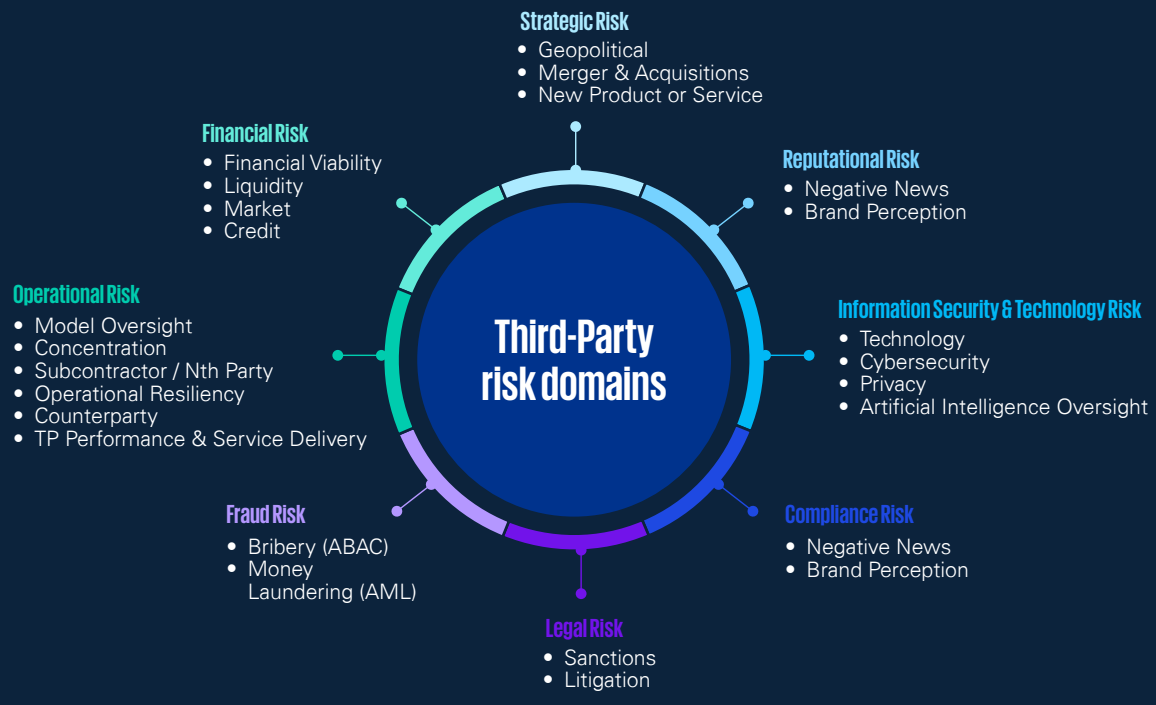
In addition to putting structures in place to address emerging risks, organizations should consider the following four imperatives for developing an effective third-party risk management program:

1 Understand the interconnected nature of third-party relationships in your ecosystem

Forty-eight percent of organizations surveyed by KPMG concede that collaboration with partners on risk management could be better, and only a quarter of respondents have a cross-functional view of risks across the enterprise.[10]

Organizations should adapt and evolve their risk management models to account for the disparate risks of their ecosystem partners and how they might intersect to create compound volatility (see Figure 1). Also, recognize what you don't know—for example, how quickly tariff and trade policies and other geopolitical risks may evolve. Regularly plan, monitor, and adapt your risk mitigation strategies and actions, particularly around issues such as shared AI vulnerabilities and data. Managing multiple variables simultaneously while aligning with business objectives requires significant attention. Ensure your governance, risk, and compliance (GRC) program expands beyond traditional lists to include risk reporting and risk monitoring technologies with advanced analytics, end-to-end value chains, and, perhaps most important, a way to analyze how risks that are interrelated can create compounded consequences.

Figure 1. How potential risks in the partner ecosystem intersect and create compound volatility



2 Implement continuous monitoring of ecosystem partners

Today, static evaluations aren't enough to mitigate third-party risks: Organizations should implement continuous monitoring and real-time intelligence feeds to best leverage data analytics to detect and respond to emerging threats and missed opportunities. In fact, in a KPMG survey, we found that 85 percent of organizations that use real-time monitoring tools, commonly used for sanction screening, negative news, and financial viability, report a significant reduction in the time it takes to detect and respond to security incidents.[11] From a risk management perspective, these capabilities allow for real-time identification of potential issues such as sanctions; cybersecurity exposures; financial instability; and compliance with local, national, and global regulations.

When it comes to missed opportunities, real-time monitoring also helps ensure that partners are constantly innovating in the name of mutual value, as opposed to simply following the terms of their contracts. To motivate this mindset in your partners, introduce managed governance that includes performance incentives for partners that go above and beyond expectations, particularly in terms of innovation.

3 Build supply chain resiliency into your ecosystem

Organizations are taking their responses to supply chain risks seriously: 71 percent of US chief executive officers plan to alter their supply chains over the next three to five years to account for regulatory changes.[12] That may not be enough: Building supply chain resilience in partner ecosystems in a way that reduces overdependency on certain partners requires a multifaceted approach. For example, diversifying supply chain partners helps ensure alternative options are available in case of disruption due to tariffs, trade wars, armed conflicts, and other geopolitical risks.

Maintaining the agility to find alternative suppliers and investing in local production to reduce import dependency can further enhance stability and control. Since ransomware groups and state-sponsored attackers are increasingly leveraging supply chains as entry points, security leaders should shift from periodic third-party reviews to real-time monitoring.[12] In addition, conduct scenario and simulated vulnerability analyses and forecasting to better anticipate where you may need to be flexible if geopolitical risks escalate, supply routes are disrupted, or shortages occur that impact one or more partners in your ecosystem.

4 Align with partners on trusted data protocols

The percentage of confirmed data breaches involving third-party relationships has doubled from 15 percent to 30 percent over the past year.[13] Despite the innovation engendered by partnerships that introduce generative AI and AI agents, bear in mind that you may also be inheriting cybersecurity and data risks through these relationships.

The percentage of confirmed data breaches involving third-party relationships has doubled over the past year.

Connecting AI-savvy partners to your internal systems can introduce risks if their cybersecurity and data privacy protocols are inadequate or if they have varying outlooks on the role humans play in technology oversight. Organizations are also concerned about the pace at which software providers—particularly in the realm of AI—are introducing new features to keep ahead of the competition.[14] Rushing products to market before robust security features are built in puts all associated partners at risk.

The sheer number of connected partners creates an expanded attack surface that bad actors can exploit in increasingly sophisticated ways, such as botnets, phishing, and adversarial attacks that target the integrity of AI input and output. Given these increased risks, organizations should align with partners on cybersecurity and data privacy standards at the outset. Further, insist that partners adhere to technical standards that elevate data protection across not only AI technologies, but also other technologies including file transfer software, industry-specific services, VPNs, and cloud infrastructure.[15] Be aware that the third-party security programs established by many cybersecurity teams are designed to align primarily with the National Institute of Standards and Technology (NIST) framework; while NIST covers a number of software vendors, they represent only a subset of all the software exposures a company and its partners might have.

Contract stipulations should include thorough specifications related to potential breaches, cyberattacks, and other disruptions. Include breach-related considerations, such as who is responsible for conducting the investigation and response, absorbing the cost, and handling business continuity. To help minimize fourth- and fifth-party threats, organizations should require partners to maintain strong third-party risk management programs of their own. Partnership agreements and contracts should be monitored, reviewed, and updated on a regular basis to account for emerging risks and help ensure that all parties are accountable for maintaining the security of the ecosystem. Conduct continuous monitoring and use advanced analytics to detect potential cyber incidents and insist that your partners do the same—practices cited by 49 percent of KPMG survey respondents as priorities.[16]

5 Leverage advanced analytics and AI for risk monitoring

AI-based monitoring tools can be indispensable for risk management. Organizations surveyed by KPMG that are using AI for risk management have seen a 60 percent improvement in their ability to predict and mitigate risks.[17] Advanced analytics and AI can process vast amounts of data, identify patterns, and provide actionable insights, enabling more informed and effective risk-management decisions. By integrating advanced analytics and AI into their risk mitigation frameworks, organizations can gain a competitive edge and better navigate the complexities of the modern business landscape.

How KPMG can help

We combine advanced technology, in-depth experience, and operational excellence to continually evolve your organization. KPMG can help you create nimble, scalable business functions that evolve alongside your organization as it grows. That helps you accelerate and sustain your transformation journey, keeping you ahead of your competitors—all while helping minimize disruption and risk. KPMG can help you:

- Identify partners, alliances, and vendors to fill capability gaps and boost your business goals
- Develop a strategy to build and manage a strategic network of partnerships and alliances
- Help to plan and manage partner ecosystems
- Evaluate the current methods and processes used for sharing data across partnerships
- Determine the anticipated increase in IT budget allocation towards enhancing the partner ecosystem

Authors

Jeanne Johnson

Principal

Jeanne Johnson is a Principal and the Global and US Customer & Operations Digital Transformation Leader in the KPMG Advisory practice with extensive experience in strategic planning, performance management, program portfolio management, business and technology architecture, and deploying new operating models. Over the last 20 years, she has helped clients navigate signficant change events such as mergers, regulatory mergers, regulatory mandates, disruptive technologies, and business transformation. Jeanne has led and delivered large-scale client solutions and data-driven transformation strategies, target operating models and roadmaps, finance information and systems strategy, architecture and design, and enterprise data strategy and competency centers. Additionally, she has led and supported KPMG development and innovation initiatives, such as data and analytics strategy and roadmap, integrated information and reporting, global business intelligence encompassing performance management, information management, and analytics, as well as vendor alliance and service integration.

Joey P. Gyengo

Principal

Joey is a Principal in the KPMG Consulting practice with over 20 years of global experience. Based in Atlanta, he is the US Enterprise Risk Management (ERM) and Third Party Risk Management (TPRM) leader and has a deep background in enterprise risk and resilience, governance, risk, and compliance (GRC), internal audit, and internal controls. Joey advises boards and senior leadership in risk strategy, risk governance, and risk management. He supports clients with their opportunities to collaborate effectively with strategy, delivering risk transformation capabilities, data-driven insights and monitoring, and integrated risk management. When not working, Joey enjoys spending time with his family and walking his daughter to elementary school. He is an avid supporter of Atlanta United, Fernbank Museum of Natural History, the Atlanta Opera, and the Auburn University School of Nursing.

We would like to thank our contributors:

The authors wish to thank Jessica Athavale, Lisa Bigelow, Donna Ceparano, Liz Kalooky, Whitney La Bounty, Matthew Miller, Mary Rollman, and Beth Wall for their contributions to this paper.

Sources

[1] Source: Accelerate growth and innovation with the right partner ecosystem, KPMG, 2025.

[2] Source: The Global Risks Report 2025, World Economic Forum.

[3] Source: Accelerate growth and innovation with the right partner ecosystem, KPMG, 2025.

[4] Source: KPMG Enterprise Risk & Resiliency Survey, 2025.

[5] Source: "Risk Management in a Technology-Driven World," Supply Wisdom, 2024.

[6] Source: Accelerate growth and innovation with the right partner ecosystem, KPMG, 2025.

[7] Source: Accelerate growth and innovation with the right partner ecosystem, KPMG, 2025.

[8] Source: Patrick Opet, "An open letter to third-party suppliers," JP Morgan Chase, 2025.

[9] Source: Victoria Bloom and Mary Frances Holland, "2025 first quarter manufacturers' outlook survey," National Association of Manufacturers, March 6, 2025.

[10] Source: Accelerate growth and innovation with the right partner ecosystem, KPMG, 2025

[11] Source: Accelerate growth and innovation with the right partner ecosystem, KPMG, 2025

[12] Source: Accelerate growth and innovation with the right partner ecosystem, KPMG, 2025

[13] Source: Global Third-Party Breach Report, SecurityScorecard, March 26, 2025.

[14] Source: Verizon Data Breach Investigations Report, April 2025.

[15] Source: Patrick Opet, "An open letter to third-party suppliers," JP Morgan Chase, 2025.

[16] Source: Global Third-Party Breach Report, SecurityScorecard, March 26, 2025.

[17] Source: Accelerate growth and innovation with the right partner ecosystem, KPMG, 2025.

For more information, contact us:

Jeanne Johnson
Principal, Advisory
jeannejohnson@kpmg.com

Joey P. Gyengo
Principal, Advisory
jgyengo@kpmg.com

Related thought leadership:

Accelerate growth and innovation with the right partner ecosystem

Intentional Collaboration: Building Partner Ecosystems for Future Growth

KPMG Risk & Resilience Survey

Trust, attitudes and use of Artificial Intelligence

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: **kpmg.com** **Subscribe**

DASD-2025-18179