As strong as your weakest link

Critical considerations in third-party risk management

July 2025
KPMG Middle East

Contents

Foreword

In today's interconnected business environment, the security chain is only as strong as its weakest link. Organizations are increasingly finding that this weak link often lies not within their infrastructure, but within the complex web of third-party relationships they have built to enhance operational efficiency and technological capabilities.

Consider the infamous SolarWinds breach of 2020. Cyber attackers stealthily embedded malicious code within a routine software update, subsequently infiltrating the networks of numerous Fortune 500 companies and prominent public-sector institutions. This event underscores a critical truth: your cybersecurity posture is as strong as your weakest third-party link.

In an increasingly interconnected global business environment, firms increasingly rely on third-party vendors for critical operations, processes, and functions. A dependency that boosts efficiency but also introduces significant cybersecurity vulnerabilities. A single weak link in the vendor chain can jeopardize sensitive data and disrupt business continuity.

Management of risks associated with third-party relationships is a top priority for management and regulatory agendas.

> **A survey conducted by KPMG found that 73 percent of respondents confirmed that inefficiencies in their TPRM program exposed them to reputational risk.**

The complexity of organizational structures and the multiple stakeholders involved in managing third-party risk remain key challenges to management teams. Based on our work as advisers to the various services industry, we have seen large firms optimize their efforts around third-party risk management (TPRM) while improving their responses to emerging risks. Regulators in the UAE and Saudi Arabia are looking into strengthening third-party risk management requirements, reflecting its increasing importance as a critical pillar of operational resilience and compliance.

This document aims to share good practices we have observed in adjusting firm programs to prioritize key risks and relationships to enhance operational resilience. By implementing a robust TPRM framework, organizations can safeguard their data assets, prevent costly breaches, and maintain compliance with evolving cybersecurity regulations. Furthermore, a strong vendor security program enhances customer confidence and ensures operational resilience.

Ton Diemont
Partner, Head of Cybersecurity — Saudi Arabia, Jordan and Lebanon

Timothy Wood
Partner, Head of Cybersecurity — UAE and Oman

Key cyber risks in third-party relationships

A company faces cybersecurity threats from vendors who manage access to its IT systems, data, and networks. The outsourcing practice, which aims to boost business efficiency, simultaneously increases the number of potential vulnerabilities. As a company employs additional vendors, its security weak points increase substantially. Understanding the most critical cyber risks in third-party relationships is essential for preventing breaches and strengthening security defenses.

01 Compliance and regulatory failures

Industries enforce strict data protection regulations that businesses must ensure their vendors follow. In 2020, Marriott International faced a US$23.8 million fine after a data breach from its third-party booking system. Non-compliance can lead to legal penalties and reputational damage, making vendor oversight essential.

02 Data breaches

Third-party relationships pose a significant risk of data breaches, exposing customer and business-sensitive information. Without strong security measures, vendors become weak links for cybercriminals. In 2023, attackers compromised an employee account at Turkish Airlines, one of Airbus's customers, gaining unauthorized access to Airbus's systems. This led to sensitive data being accessed, highlighting vulnerabilities in the supply chain.

03 Supplier concentration risks

Across sectors, there is an increase in supplier concentration, which raises dependency and competition concerns. With the move towards digital transformation and cloud implementation, this connected and concentration risk has accelerated and will continue to do so.

04 Poor incident response and vendor communication

Delays in breach notifications worsen cyberattack impacts. Vendors must promptly inform clients to prevent further damage. In 2021, a Facebook cyberattack exposed 503 million user records, but inadequate communication left users unaware of their compromised data. Effective incident response and transparent vendor communication are crucial to minimizing security risks.

05 Supply chain attacks

In 2025, hackers affiliated with Russian military intelligence targeted Western firms involved in shipping aid to Ukraine. Over 10,000 internet-connected cameras near Ukrainian borders were targeted to gather intelligence on aid shipments.

06 Insider threats

Cyber risks aren't limited to external hackers—insider threats from vendors' employees and contractors can lead to data theft, sabotage, or fraud. In 2020, a former Cisco employee deleted 16,000 WebEx accounts, disrupting operations. Organizations must enforce strict access controls and continuous monitoring to mitigate insider threats.

07 Lack of visibility and control

Many organizations struggle to monitor vendor security practices, increasing their exposure to cyber threats. According to Gartner, businesses often lack standardized third-party risk management frameworks, making it difficult to assess and control cybersecurity measures. Improved visibility and proactive oversight are essential for mitigating third-party risks.

Case studies:

Cyber risks in third-party relationships

Real-world incidents highlight how third-party vulnerabilities can lead to security breaches and financial losses. The following case studies illustrate the impact of cyber risks on vendor relationships and key lessons learned.

Lessons from the CDK Global attack

A software provider for nearly 15,000 North American car dealerships, CDK Global, suffered a ransomware attack in 2024. The attack disrupted operations across numerous dealerships, emphasizing the risks in the automotive supply chain.

Third-party risk in healthcare

In 2024, Change Healthcare, a major health payment processing company, was hit by a ransomware attack. Operations were disrupted and up to 6TB of sensitive patient data was stolen, affecting millions.

98%

of organizations have a relationship with at least one third-party that has experienced a breach in the last two years.

Source: Cyentia Institute and SecurityScoredcard

Common challenges in third-party risk management

Managing third-party cybersecurity risks presents several obstacles for businesses. Some are technical, others are organizational. All require strategic planning.

01 Lack of visibility into third-party security practices

Many vendors do not disclose their full security posture. Some lack proper security controls, while others hesitate to share details. Businesses often rely on questionnaires and self-assessments, but these are not always accurate. Without direct visibility, risk assessment becomes unreliable.

02 Inconsistent risk assessment processes

Many organizations lack a standardized method to assess third-party risk before onboarding or periodically afterward. Risk assessments are sometimes limited to initial due diligence, with no ongoing evaluation.

03 Resource constraints for small and medium-sized enterprises

Large enterprises have dedicated TPRM teams. SMEs, on the other hand, often lack the budget and staff for specialized risk oversight. Many must rely on general IT teams to handle vendor security, leading to gaps.

04 Managing risks across complex supply chains

Multinational companies work with thousands of vendors. Many of these vendors also rely on subcontractors (fourth parties), further complicating oversight. As a result, vendors might be onboard without proper risk evaluation.

05 Balancing security with business agility

Stronger security controls reduce risk, but they can also slow down vendor onboarding. Extensive security reviews and compliance checks delay partnerships, affecting time-sensitive projects. Finding the right balance between security and operational efficiency is difficult but necessary.

06 Insufficient contractual controls

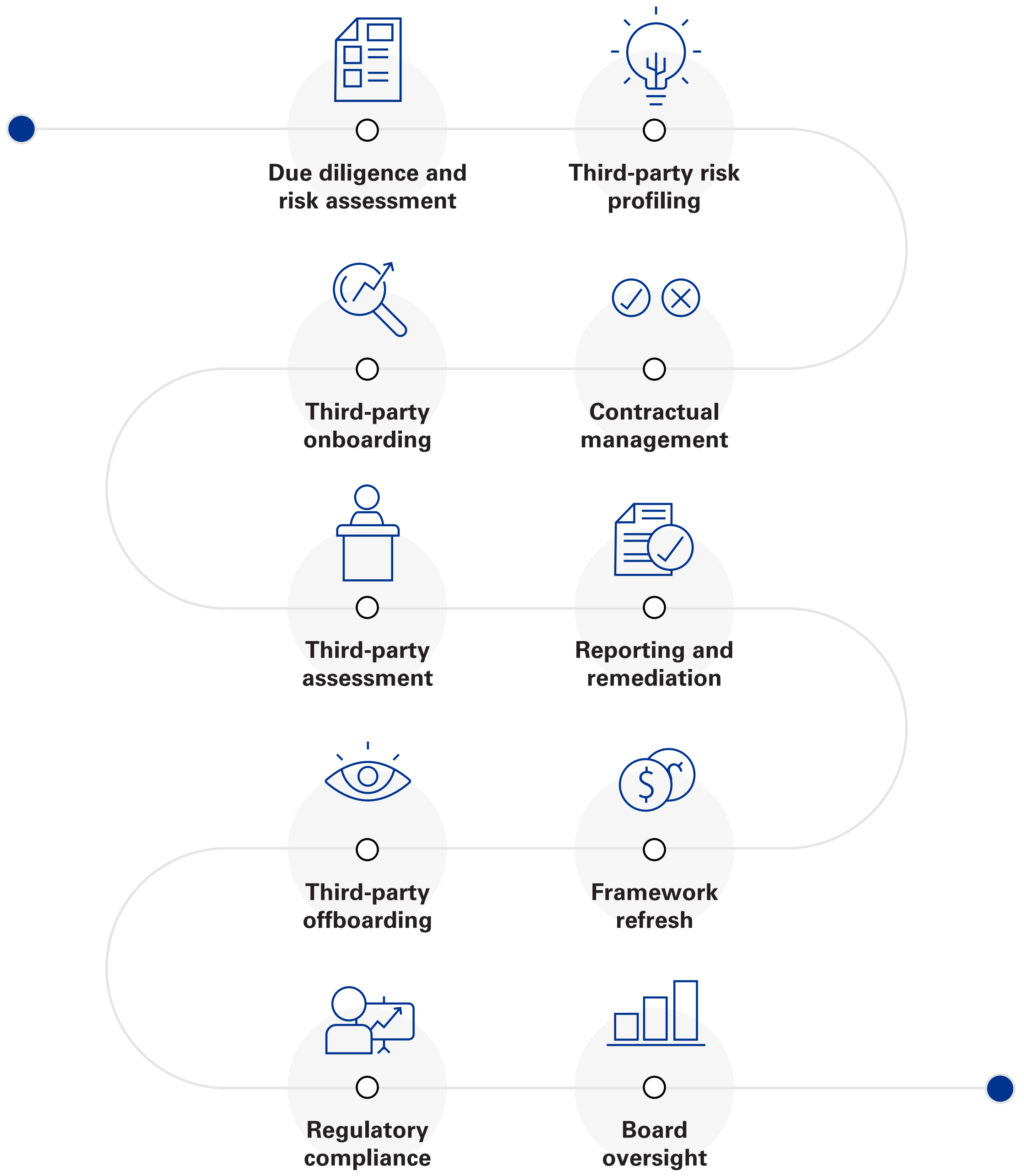
Contracts may lack clear security expectations, service-level agreements (SLAs) or clauses for incident reporting, data protection, and audits. Failure to define these terms can lead to gaps in compliance and accountability.

Identifying and managing third-party cyber risks:

Good practices for effective risk management

Mitigating third-party cyber risks requires a structured and well-governed approach. Organizations must evaluate vendors before onboarding, define clear cybersecurity expectations within contracts, and implement continuous monitoring throughout the engagement lifecycle.

We emphasize that an organization's ability to effectively mitigate third-party risks depends on the maturity of its internal processes and governance structure. This approach should include key steps such as:



Due diligence and risk assessment

Third-party risk profiling

Third-party onboarding

Contractual management

Third-party assessment

Reporting and remediation

Third-party offboarding

Framework refresh

Regulatory compliance

Board oversight

The future of TPRM:

Trends and emerging challenges

Third-party risks are evolving fast. Businesses need to adjust their operations because new threats, technological advances, and regulatory requirements appear rapidly.

New tech brings new risks

Cloud, AI, IoT, and blockchain create fresh challenges. AI attacks can strike on their own. IoT devices open new weak spots, especially in factories and hospitals. Blockchain helps secure vendor data with unbreakable records.

Rules keep changing

Organizations face growing regulatory demands to strengthen their third-party risk management practices. For example, the EU's Digital Operational Resilience Act (DORA) requires financial institutions to enhance vendor cybersecurity oversight and ensure operational resilience across their supply chain.

Cyber insurance grows

More businesses buy cyber insurance to cover vendor breaches. But insurers now demand stronger risk controls first.

Zero trust takes over

Companies now use Zero Trust models. Vendors must prove they are safe all the time. This stops data breaches by limiting vendor access.

How generative AI is transforming third-party risk management

Based on our work with clients, generative AI (GenAI) has come out with the potential to significantly reshape both procurement's operating model and how organizations assess and manage third-party cyber risks. As GenAI capabilities mature, procurement and cybersecurity teams alike will benefit from intelligent assistants that offer continuous support, surfacing deeper insights into supplier ecosystems, identifying emerging risks, and enhancing overall resilience.

Initial analyses suggest that 50 to 80 percent of today's procurement tasks, including many linked to vendor risk evaluations, can be automated, streamlined, or shifted to self-service models. Accor By embedding GenAI across procurement and third-party risk processes, organizations stand to improve their return on investment, negotiate more effectively, and elevate their influence in strategic decision-making—all while better protecting sensitive data and minimizing cyber exposure.

GenAI can transform third-party cyber risk management by automating complex diligence tasks, such as contract intelligence, data privacy assessments, and supplier compliance checks. These tools can analyze large volumes of structured and unstructured data, scanning for regulatory misalignments, identifying security gaps in vendor documentation, or flagging inconsistencies in responses to cyber risk questionnaires.

As AI integrates more deeply with enterprise risk management frameworks, organizations can dynamically reassess vendor risk profiles in response to real-time cyber threats or supply chain disruptions. GenAI can reduce operational costs and elevate procurement's strategic role in enterprise cyber resilience, ensuring that organizations are better prepared to detect, assess, and respond to the evolving risks introduced by third parties.

Examples of GenAI use cases in TPRM

- 01 Automated third-party risk assessments
- 02 Security questionnaire automation
- 03 Contract and SLA cyber clause review
- 04 Continuous risk monitoring
- 05 Regulatory compliance mapping
- 06 Supply chain threat modeling
- 07 Incident simulation
- 08 AI-driven vendor intelligence reports
- 09 Anomaly detection in procurement activities
- 10 Streamlined onboarding

A model for the future

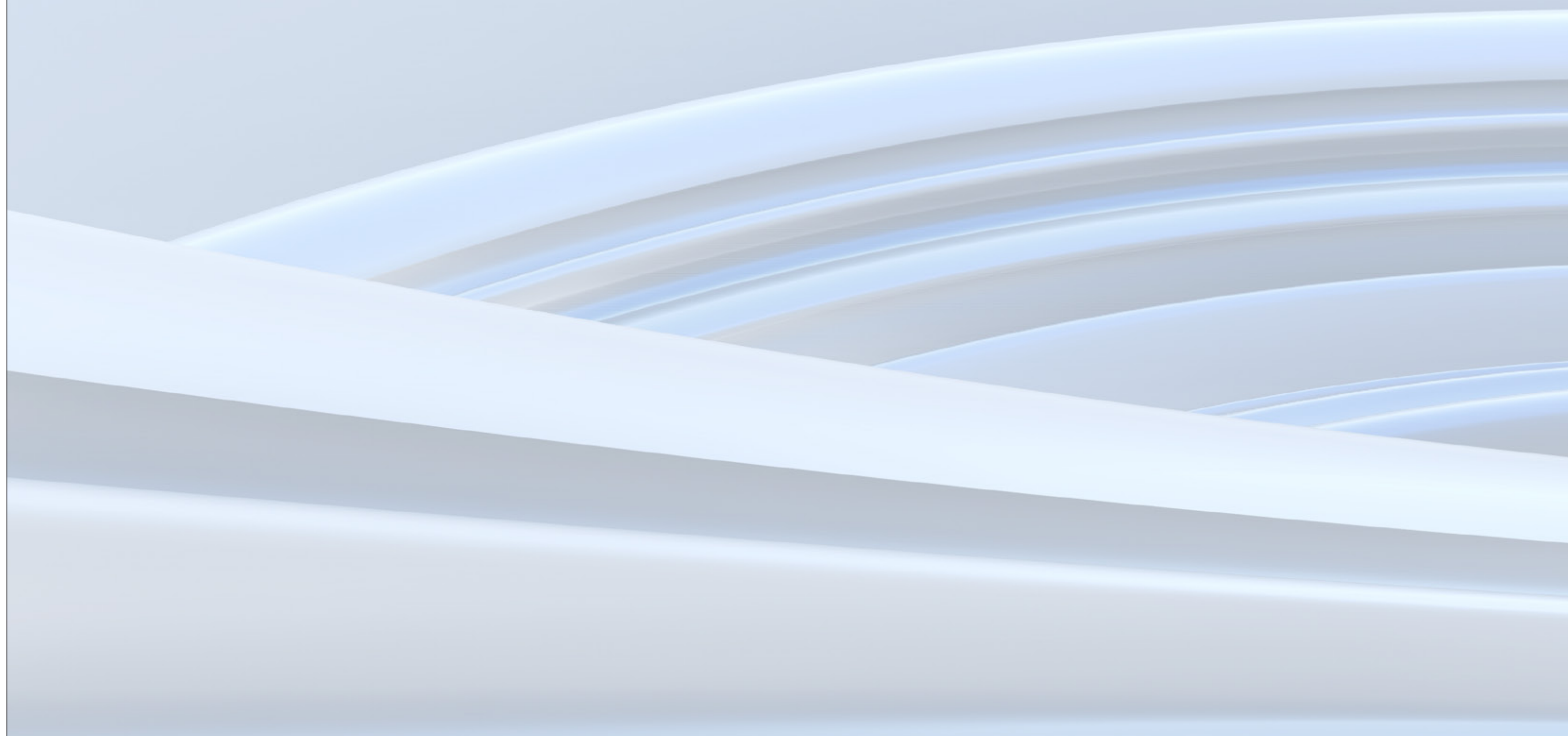
In an increasingly connected digital landscape, one organization stood out—not because it avoided third-party relationships, but because it mastered how to manage them. With a growing web of vendors, suppliers, and service providers, the company recognized early on that its cybersecurity posture was only as strong as its weakest link.

Instead of waiting for an incident to strike, it adopted a structured TPRM framework. This included:

- Carefully evaluating each vendor based on their risk profile
- Mapping risks and clearly assigning responsibilities
- Implementing targeted controls
- Replacing one-time assessments with continuous monitoring
- Embedding resilience as a daily operational habit, not just a crisis response

As regulations tightened and supply chain attacks made headlines, this organization didn't scramble—it adapted with confidence. By being proactive, it didn't just prevent breaches or pass audits—it built trust. Stakeholders, partners, and customers recognized a business that took security seriously, not just for itself, but for everyone it touched.

This isn't just a success story—it's a model for the future. Because in a world full of digital dependencies, resilience isn't optional. It's earned—one third-party risk at a time.



Contacts

Ton Diemont
Partner, Head of Cybersecurity — Saudi Arabia, Jordan and Lebanon
KPMG Middle East
antondiemont@kpmg.com

Timothy Wood
Partner, Head of Cybersecurity — UAE and Oman
KPMG Middle East
timothywood@kpmg.com

Arbab Chaudhry
Director, Cyber Strategy and Governance
KPMG Middle East
arbabchoudhary@kpmg.com

Mohammed Alshaghdali
Associate Director, Cybersecurity, TPCRM Lead
KPMG Middle East
malshaghdali@kpmg.com

Contributor

Brienish Alva, Associate Director, Cybersecurity
Abhimanyu Shandilya, Manager, Cybersecurity
Syed Ahmed, Assistant Manager, Cybersecurity

kpmg.com/sa
kpmg.com/ae
kpmg.com/om
kpmg.com/jo
kpmg.com/lb

Disclaimer

KPMG is a global organization of independent professional services firms providing Audit, Tax and Advisory services. KPMG is the brand under which the member firms of KPMG International Limited ("KPMG International") operate and provide professional services. "KPMG" is used to refer to individual member firms within the KPMG organization or to one or more member firms collectively.

KPMG firms operate in 142 countries and territories with more than 275,000 partners and employees working in member firms around the world. Each KPMG firm is a legally distinct and separate entity and describes itself as such. Each KPMG member firm is responsible for its own obligations and liabilities.

KPMG International Limited is a private English company limited by guarantee. KPMG International Limited and its related entities do not provide services to clients. For more detail about our structure, please visit kpmg.com/governance.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.