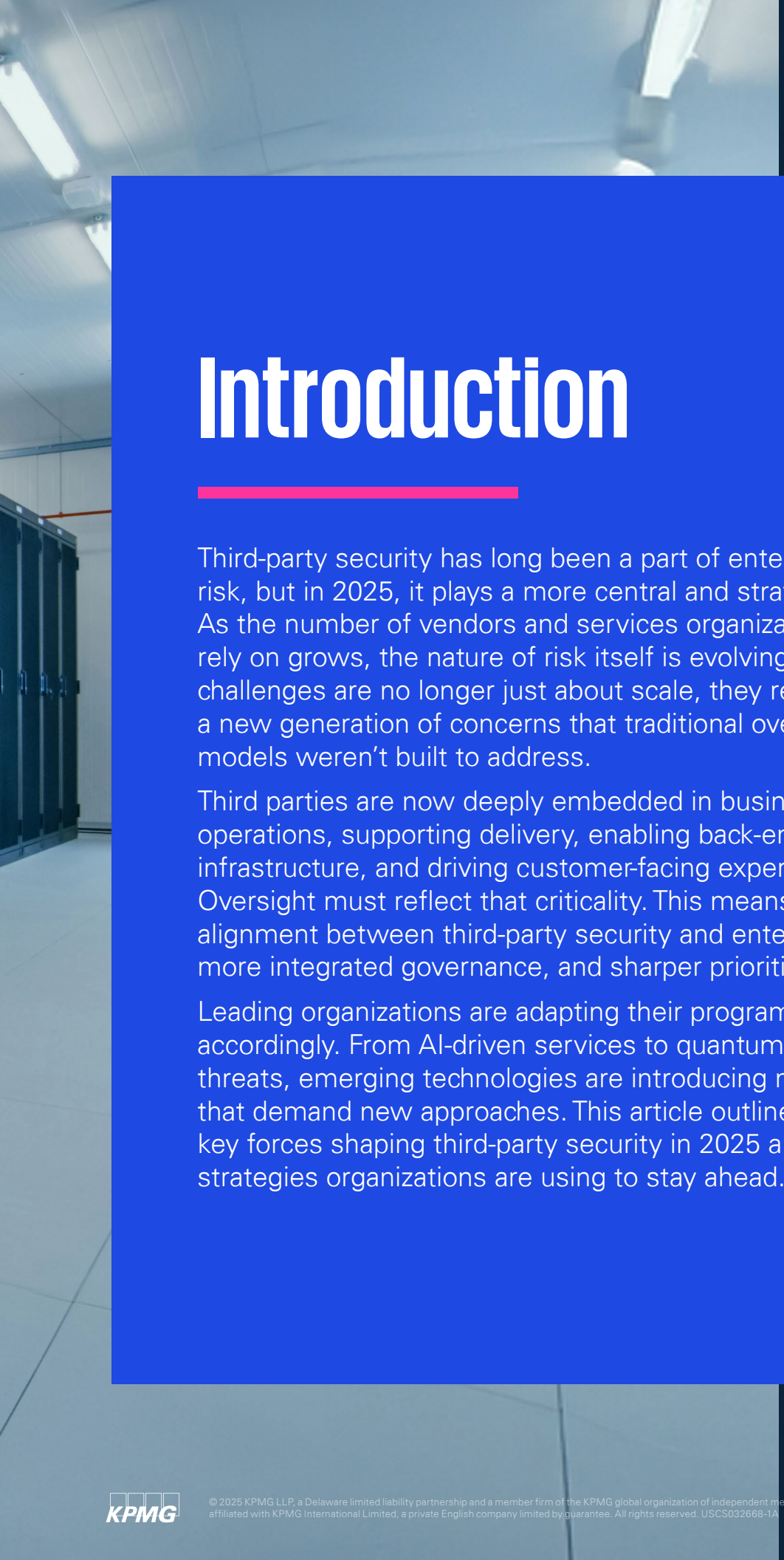
KPMG

2025 Key considerations in third-party security

kpmg.com



Introduction

Third-party security has long been a part of enterprise risk, but in 2025, it plays a more central and strategic role. As the number of vendors and services organizations rely on grows, the nature of risk itself is evolving. The challenges are no longer just about scale, they reflect a new generation of concerns that traditional oversight models weren't built to address.

Third parties are now deeply embedded in business operations, supporting delivery, enabling back-end infrastructure, and driving customer-facing experiences. Oversight must reflect that criticality. This means closer alignment between third-party security and enterprise risk, more integrated governance, and sharper prioritization.

Leading organizations are adapting their programs accordingly. From AI-driven services to quantum-era threats, emerging technologies are introducing new risks that demand new approaches. This article outlines the key forces shaping third-party security in 2025 and the strategies organizations are using to stay ahead.

Key drivers of integrated TPS within TPRM and the broader organization

As third-party security becomes more embedded in core operations, organizations are shifting from isolated control checks to more integrated, strategic oversight. Three primary drivers are shaping this evolution: vendor population reduction, trade and regulatory complexity, and stronger cross-functional alignment.

Reducing vendor count can simplify oversight and reduce exposure. Fewer relationships mean lower administrative burden, tighter control, and fewer points of entry for threat actors. But consolidation must be done thoughtfully. Organizations still need redundancy, specialized capabilities, and geographic coverage. Effective programs balance strategic reduction with operational resilience.

Global trade dynamics also now carry direct security implications. Tariffs, data sovereignty requirements, and regional instability are influencing sourcing decisions. Security teams are increasingly involved in evaluating the downstream risk of those decisions, ensuring that shifts in vendor location or ownership don't introduce compliance or threat exposure.

Integrated third-party security also depends on collaboration across functions. When procurement, IT, legal, and security operate in silos, vendors may be onboarded or offboarded without adequate controls. Leading organizations are establishing cross-functional governance to evaluate vendors holistically, embed shared success measures, and align third-party security with broader enterprise risk strategy.

Responding to regulatory pressure: DORA and NIS2

New EU regulations, DORA (Digital Operational Resilience Act) and NIS2 (the second Network and Information Security Directive), are reshaping how organizations manage third-party risk. These directives go beyond traditional compliance and require organizations to demonstrate accountability, resilience, and continuous oversight. But while the expectations are clear, much of the operational guidance is not.

Both frameworks introduce the concept of "critical third parties" without specifically defining a methodology for who qualifies. Under DORA, financial institutions must evaluate ICT (Information and Communication Technology) providers—such as cloud services, cybersecurity vendors, and data centers—for systemic importance and concentration risk. NIS2 requires essential entities to ensure cybersecurity protections across all external dependencies. This shifts responsibility to organizations to establish their own definitions, based on service impact, data sensitivity, and substitution risk.

Oversight expectations are rising in parallel. DORA mandates real-time monitoring, incident reporting, and audit rights. NIS2 reinforces that even if vendors operate outside the regulatory perimeter, the organization is still accountable for ensuring their controls. Static assessments are no longer sufficient.

Perhaps most importantly, these frameworks elevate third-party security to a board-level concern. Management teams are expected to understand third-party exposure and lead coordinated responses. This has driven demand for stronger internal governance, more specific contract language, and a clearer view of enterprise risk posture. Programs built for checkbox compliance will struggle to meet these evolving demands.

Using AI to drive efficient and effective third-party security

AI is beginning to reshape third-party security, not just by increasing efficiency, but by improving how risk is interpreted and prioritized. Many early deployments focused on automating manual tasks, such as parsing documentation or triggering workflows. These delivered speed, but not necessarily insight.

Now, organizations are turning to more advanced uses of AI to make sense of the growing volume of vendor data. Predictive analytics can flag vendors at heightened breach risk. Anomaly detection can surface deviations in vendor behavior or data exchange. Real-time processing enables faster recognition of emerging threats. Together, these tools help shift programs from reactive oversight to proactive control.

Leading organizations are exploring agentic-AI-systems that can make decisions within predefined parameters. In a third-party security context, this might mean recommending risk mitigation actions or escalating issues without human input. While promising, these approaches must be built with transparency and guardrails in mind. Otherwise, they can risk introducing new uncertainty rather than resolving it.

As the vendor landscape becomes more complex, AI is not a silver bullet, but it is becoming a critical layer in how organizations surface, contextualize, and act on third-party risk.

Securing against third-party AI risk

As vendors embed AI into their products and services, organizations are inheriting risk they didn't create and can't always see. From foundational models powering customer tools to AI-enhanced decision systems, third-party AI use is now common, and its associated risks increasingly material.

These risks span privacy, ethics, and operations. Sensitive data may be processed or retained in ways that violate expectations. Models may generate biased or unreliable outputs that damage reputation or impact business decisions. Retraining cycles, often opaque, can alter system behavior with no notice. And because most of these models are vendor-developed, visibility and governance are limited.

Leading programs are adapting. Rather than simply asking whether AI is used, they are evaluating how it's embedded, what data it touches, and what could go wrong. This has influenced risk tiering, due diligence scope, and contract structure. Some organizations are now requiring documentation around training data, testing protocols, and human oversight, and ensuring technical rights to audit or remediate are incorporated where feasible.

Monitoring tools are evolving as well. AI usage discovery platforms and output analysis engines help organizations identify how vendor models behave over time, especially when use is undeclared or has changed post-onboarding. And in some cases, AI is helping secure AI, supporting anomaly detection and surfacing risk signals that would otherwise go unnoticed.

The baseline expectation has changed: third-party AI risk is no longer edge-case, it's part of the modern risk surface.

Third-party quantum risk

Quantum computing is no longer theoretical. With active investments across public and private sectors, the threat of quantum-enabled decryption, harvest-now and decrypt-later, is becoming real. Sensitive data encrypted today may be compromised in the future if stored by a third party and accessed with quantum-capable tools.

This changes the calculus of risk. Organizations must assess the "shelf life" of their sensitive data and determine which vendors present long-term exposure. Data that must remain confidential over a decade, such as customer records, financial data, or IP (intellectual property), requires post-quantum protections now, not later.

The first step is prioritization. Not all third parties pose equal quantum risk. Programs must evaluate vendors based on data sensitivity, duration of storage, and cryptographic hygiene. Once identified, these vendors should be assessed for readiness using maturity models or targeted questionnaires—such as the FS-ISAC PQC (Post-Quantum Cryptography) Vendor Questionnaire or the Wells Fargo PQC Maturity Framework.

Implementing post-quantum cryptography is not trivial. It's costly, complex, and disruptive. Organizations that apply it universally will overspend, those that delay entirely will fall behind. Modeling techniques and AI tools can help identify where controls are most needed, applying quantum-safe standards where they matter most.

Quantum risk isn't widespread yet, but for high-value, long-duration data, it's already actionable.

Monitoring third-party signals to enable real continuous oversight

Traditional third-party programs have relied on scheduled assessments to track vendor performance. But as third-party environments evolve more rapidly, that cadence is increasingly inadequate. Leading organizations are moving toward continuous monitoring, using real-time signals to surface emerging risks and trigger early intervention.

This shift requires more than new tools, it requires a new view of what's worth monitoring. Risk teams are layering internal controls with external indicators, such as credential leaks, financial distress signals, or inconsistencies in disclosures. These signals offer high-context clues that a vendor's posture may be shifting, well before a formal reassessment is due.

The most mature programs link these signals directly to action. If a vendor's behavior suggests risk, that insight feeds into governance workflows: contract reviews, escalation paths, or targeted remediation. Without that connection between signal and consequence, monitoring risks becoming noise.

Platform support is also expanding. Solutions now analyze observable behaviors, patch hygiene, access management, web exposure, and pair those insights with internal benchmarks. Some even tap underground data sources to flag high-risk activity.

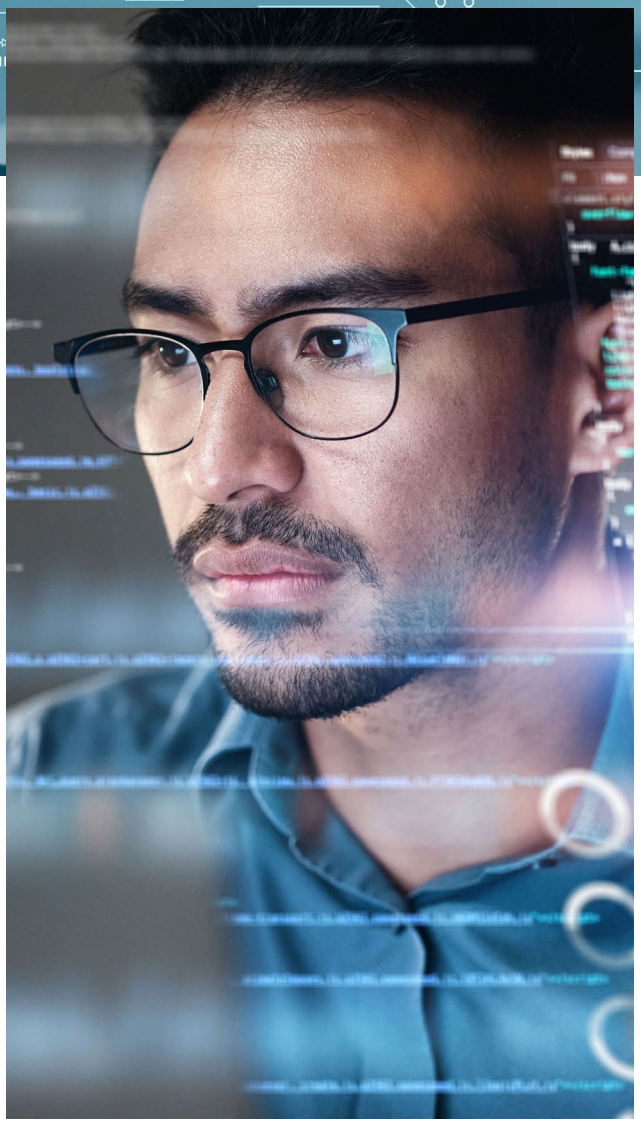
As vendor ecosystems grow in complexity and scale, the ability to detect change early has become essential. Continuous monitoring is no longer optional, it's foundational to modern third-party risk management.

Conclusion

Third-party security is no longer a back-office function, it's a strategic discipline shaping enterprise resilience. As technologies evolve and regulatory pressure grows, programs must do more than respond to risk. They must anticipate it.

Across all six themes explored in this piece, a pattern emerges: successful organizations differentiate their oversight, embed risk thinking early in vendor engagement, and align governance across legal, IT, procurement, and executive leadership. They scale their programs not just with tools, but with clear strategy, repeatable decision-making, and real-time adaptation.

As the landscape continues to shift, from AI and quantum to global regulation and market volatility, those that evolve now will be positioned to lead. Third-party security has become a defining capability of enterprise risk. Leading programs will be defined not just by the scale of their oversight, but by the precision and confidence of their decisions.



Contact us

Diana Keele
Managing Director
KPMG LLP
T: 602-203-9004
E: dkeele@kpmg.com

Chetan Gavankar
Principal
KPMG LLP
T: 339-206-3913
E: cgavankar@kpmg.com

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

Learn about us: kpmg.com