Navigating Third Party Risk Management in the digital and geopolitical era

Strategies for resilience and compliance

Management Summary

In today's rapidly evolving digital and geopolitical landscape, Third Party Risk Management (TPRM) has become a critical concern for organizations aiming to ensure resilience, compliance, and strategic advantage. This white paper explores how the boundaries of corporate responsibility have expanded: companies are now accountable not only for their own actions but also for the conduct and resilience of third parties, such as their suppliers, service providers, and digital platforms. This shift is driven by societal expectations, increasingly complex value chains, and a surge in regulatory requirements. The European Union's Digital Decade agenda exemplifies this trend; with the introduction of several new digital laws and regulations such as the Digtal Servies Act (DSA) Digital Operational Resilience Act (DORA), the Network and Information Security Directive 2 (NIS2), and the Artificial Intelligence Act (AI Act). These regulations transfer liability from third parties to the organizations themselves, making it essential for companies to embed robust TPRM frameworks into their governance, contracts, and daily operations.

This paper highlights the urgency of moving TPRM from a back-office control to a board-level mandate. It describes how fragmented data, siloed processes, and unclear ownership can leave organizations exposed to legal, operational, and reputational risks. The challenges are compounded by the pace of regulatory change, the unpredictability of geopolitical events, and the growing threat of cyber incidents. Many organizations struggle with over-reliance on static assessments, lack of real-time monitoring, and insufficient contingency planning, all of which can undermine their ability to respond to disruptions and regulatory demands.

To address these challenges, the white paper presents a practical framework for building and elevating TPRM. It advocates for embedding TPRM into governance, contract lifecycle management, and procurement processes, ensuring that risk, legal, security, and business owners share clear accountability. Standardizing and automating due diligence, monitoring, and incident response are furthermore explored as ways to deliver continuous assurance and support adoption of new regulatory requirements. The use of data, technology, and AI tools are noted to improve supplier visibility, risk assessments, and operational efficiency, while harmonizing oversight and contractual controls help organizations scale their TPRM efforts across jurisdictions.

The strategic benefits of proactive TPRM are substantial. Organizations that act now can shorten procurement lead times, improve negotiating leverage, and enhance their resilience in the face of growing supply chain, cyber, and geopolitical disruptions. Effective TPRM additionally strengthens brand trust and enables companies to turn compliance efforts into sources of strategic value. The paper provides actionable steps for organizations at any stage of their TPRM journey, including aligning regulatory requirements with strategic objectives, engaging stakeholders, building a business case for value protection, streamlining onboarding and maintenance processes, in addition to embedding automation and efficiency into TPRM practices.

Ultimately, this paper calls for a shift from reactive, compliance-driven TPRM to a proactive, strategic approach that delivers resilience and unlocks value. Organizations that embrace this transformation will not only meet regulatory demands but also position themselves for sustained growth and success in an unpredictable world.

Contents

The "why now"

Corporate integrity now appears to extend beyond a company's own actions and is increasingly assessed based on the conduct of the company's third parties. In our interconnected economy, third-party suppliers, service providers, data processors, and platforms shape operational resilience, legal exposure, and reputation. The regulatory shift of liability from third parties to the organisations that rely upon them creates an urgent need to act. Under the EU's Digital Decade framework, companies can no longer disclaim responsibility for risks outsourced to vendors, platforms, or ICT providers. Instead, liability increasingly attaches to the company itself, even when risks originate in the supply chain. For example, the Digital Operational Resilience Act (DORA) requires financial institutions to assume responsibility for the operational resilience of their ICT providers, while the Digital Services Act (DSA) imposes direct liability on platforms for ensuring trader verification and transparency. This trend signals a structural realignment: organisations are expected to take on more liability than before, embedding vendor accountability into their own governance, contractual, and operational frameworks.

As societal expectations rise, value chains fragment, and regulation accelerates. Third-party Risk Management (TPRM) has shifted from a back-office control to a board-level mandate. The imperative now is not whether to act, but how swiftly to integrate a proactive and scalable TPRM strategy. This shift has direct implications for the obligations and potential liabilities of board members. Companies and their boards are now expected to exercise heightened oversight of their third-party relationships, ensuring that robust TPRM frameworks are in place and that compliance with evolving regulations, such as DORA, Network and Information Security Directive 2 (NIS2), and the Artificial Intelligence Act (AI Act), is continuously monitored and enforced, not just their internal operations. Failure to do so may expose companies and their board members to regulatory sanctions, civil liability, or reputational harm if these third-party failures result in breaches of law or operational disruptions.

Imagine a scenario where a company relies heavily on a third-party ICT provider for critical infrastructure and services. During a routine audit, it is discovered that this provider has not met the operational resilience standards required under the DORA. As a result, the institution is vulnerable to disruptions that could lead to significant financial losses and damage to client trust. This compliance gap exposes the institution to substantial penalties and legal liabilities while diminishing the confidence of clients and stakeholders who expect seamless service and stringent data protection. In addition, the board is compelled to address these vulnerabilities publicly, which could lead to intensified regulatory scrutiny and a tarnished industry reputation. This scenario illustrates the importance of a robust TPRM strategy, emphasizing the need for continuous oversight and compliance verification of third-party vendors to ensure that all regulatory demands are met.

Although TPRM covers various laws, including sustainability measures such as the Corporate Sustainability Due Diligence Directive (CSDDD), this paper focuses on key challenges and opportunities from the EU's Digital Decade as a crucial aspect of regulatory change. While acknowledging the importance of other key areas, the following discussion will concentrate specifically on the digital landscape to provide a more targeted analysis.

Several forces are converging:

Accountability beyond the company: Stakeholders expect companies to monitor and continuously oversee the ethics, security, and compliance of their third-party partners, not just their internal operations.

Fragile, complex supply chains: Geopolitics, cyber incidents, and concentrated dependencies expose single points of failure. Procurement cycles lengthen amid re-contracting and complex ICT negotiations; a pain point amplified under regimes such as DORA (as highlighted by recent industry research).

Regulatory acceleration: The EU's Digital Decade is redefining obligations across cybersecurity, data, intermediaries, product and services and AI. The DSA applies since February 2024, the NIS2 since October 2024 and is still being transposed into national laws, the DORA applies since January 2025, and the AI Act and Data Act phase in over the next two years. Compliance is shifting from "go-live" exercises to continuous, auditable governance of third-party dependencies. Many of these laws overlap across common subject areas, which calls for moving away from a siloed, law-by-law approach toward an integrated implementation framework.

Internal gaps: Divergent regulations, uneven automation, limited visibility across tiers, unclear ownership of TPRM and lagging governance structures create fragmented responses and duplicated effort.

If left unaddressed, these dynamics translate into higher costs, delays in realizing time-to-value, and escalating legal and reputational risk. Concentration risk builds as a small set of providers anchor critical processes without sufficient contingency. Sensitivity and exposure to geopolitical disruption mounts through reliance on agents outside of the company's sphere of influence. Gaps in supply chain visibility obscure upstream and sub-tier exposures. Contracting drags as organisations reinvent terms for each regulation, and compliance becomes episodic rather than evidenced in real time. The result is a reactive, "just-in-time" approach unsuited to the pace and complexity of today's environment. The imperative is to move to a proactive, "just-in-case" model that makes resilience a design principle. Practically, that means:

- **Embedding TPRM into governance and procurement** so risk, legal, security, and business owners share clear accountability.
- **Standardising and automating due diligence, monitoring, and incident response** to deliver continuous assurance, not periodic snapshots.
- **Building harmonised, contractually enforceable oversight**, clauses, controls, and data-sharing obligations that scale across jurisdictions and laws and can absorb new rules without repeated structural change.
- **Improving data portability and supplier interchangeability** to reduce lock-in, accelerate switching, and foster competition.
- **Using risk-based segmentation to safely engage higher-risk providers** where they deliver strategic value, backed by mitigating controls.

Regulation highlights the urgency for action. Supervisors are powering up to a European multi-layered regime, moving from checklist compliance to evidence-based oversight. Under NIS2, organisations are expected to manage supply-chain security as part of essential service delivery.

DORA requires continuous monitoring of critical ICT third parties and operational resilience. The, DSA, AI Act and Data Act will moreover recalibrate vendor obligations, data access rights, and contractual terms. Companies that delay action on compliance with the new laws and regulations under the Digital Decade risk not only fragmented remediation and challenging audit findings but also face potential fines, service disruptions, board-level liability, and significant reputational damage, especially as these frameworks explicitly mandate that organisations ensure their third-party vendors and partners meet all relevant standards. Those that prepare can ensure continuous compliance, minimize disruption, and strengthen their negotiating position.

The strategic benefit of enhanced TPRM processes is substantial. Effective TPRM shortens procurement lead times, improves negotiating leverage, can mitigate vendor and supply chain disruptions, and reduces the total cost of risk. It enables faster pivots when markets, technologies, or regulations shift. It strengthens brand trust by supporting evidencing of responsible ecosystem choices. Most importantly, it turns compliance efforts into durable capabilities: governance, processes, and a data foundation that supports transformation rather than slowing it.

This paper presents a practical framework to operationalise the shift toward harmonised and adaptive third-party oversight by focusing on governance, processes, tooling, data models, and contractual templates, see page 12. The aim is to support demonstrable resilience, actionable agility, and achieving a competitive edge that strengthens as regulatory standards advance. By proactively embedding these core principles, firms can successfully navigate the evolving Digital Decade while maintaining broader integrity and accountability across all third-party relationships.

Setting the scene: how companies need to work in a volatile world

Companies today find themselves navigating persistent volatility. Strategic partnerships with suppliers, service providers, and collaborators, now directly determine resilience, continuity, and the capacity to navigate disruption. Grasping the dynamics of these third-party relationships has become crucial to achieving strategic objectives. The case for deeper insight into third-party relationships is driven by an interlinked set of topics: geopolitical shifts, technology concentration, supply fragility, escalating cyber threats, and an evolving regulatory landscape. Together, they create a web of dependencies and risks that must be managed coherently rather than in silos.

The strategic context

In a world characterised by heightened uncertainty, and shaped by these interlinked topics, organisations require a comprehensive view of their third-party ecosystem. Examining third-party dynamics enables firms to mitigate risk, seize opportunities, and adapt to evolving conditions. Transparency and robust due diligence are foundational to providing a unified approach to managing geopolitical exposure, technological dependencies, supply chain vulnerabilities, cyber risks, and regulatory change as part of a single, integrated approach.

Practically, achieving this begins with clarity on criticality and interdependence. Organisations will benefit from identifying which third-parties underpin essential services and strategic initiatives, and how those relationships connect across business units and regions. Beyond a static roster, this means mapping functional dependencies (what fails if a provider fails), understanding tier-two and tier-three exposures, and acknowledging concentration risks derived from reliance on a few key providers. This visibility enables prioritisation of due diligence and monitoring efforts where the impact is most significant, rather than evenly distributing resources across the entire supplier base. Diversification of and insight into suppliers will enable you to reduce supplier concentration at lower cost and potentially facilitate more effective response to disruptions.

Achieving a comprehensive understanding of third-party suppliers also necessitates shared ownership among procurement, risk management, security, legal, and business leaders, each of whom has a different perception of third-party risk. Without alignment between these groups controls can become fragmented and inefficient. By integrating these perspectives, operational expectations, and risk controls can reinforce one another. This transforms due diligence from a mere compliance exercise into decision making. This approach facilitates earlier stress detection, quicker re-negotiations and more effective contingency planning. Additionally, maintaining an appropriate assessment cadence is crucial: periodic checks alone are insufficient in a volatile environment. Establishing a continuous review process with clearly defined triggers, such as significant incidents (e.g., material incidents, geopolitical developments, regulatory changes), keeps focus on the most critical third-party relationships.

Furthermore, diversifying supplier ecosystems in both logistics and cyber is an effective, and trending, method to mitigate geopolitical risk but requires increased third-party management skills to maintain overview, agility, and compliance. Through solid TPRM programmes, insight is gained into where an organisation's sphere of influence ends and where its reliance on outside providers begins, allowing for sharper scenario planning and risk mitigation strategies.

The board also plays a crucial role in guiding strategy and aligning management with business objectives. The following questions may be used to encourage board members to critically assess TPRM strategies and engage senior leaders in risk and procurement.

Five questions for the board:

- How do we **identify and prioritise the third-party relationships** that are truly critical to our operations?
- What **mechanisms provide continuous monitoring of third-party compliance** with our risk management policies?
- How do we **ensure that suppliers and partners align with our cybersecurity standards and practices?**
- Are we **prepared to respond quickly to geopolitical shifts and regulatory changes** that affect our third parties?
- How are we **reducing concentration risk and single points of failure,** including through diversification and contingency plans?

By addressing these questions, boards can guide their organisations toward proactive risk management, supporting resilience and competitiveness.

A connected risk picture

Geopolitical risks now materially influence where and how companies operate. Sanctions volatility, export controls, tariffs, and post-pandemic trends toward decoupling, friendshoring, and nearshoring are reshaping supply chains and market access. Reconfiguring toward "friendly" jurisdictions can reduce exposure but requires recalibrating existing third-party engagements and contracts, sometimes at short notice. The practical challenge is balancing continuity with agility: maintaining service levels while adapting both vendors and routes as conditions change. This calls for a clear view of which third-party providers are most exposed to geopolitical shifts and what alternatives exist, so that changes can be sequenced without disrupting operations.

At the same time, technology concentration creates systemic dependencies. Reliance on cloud services, telecommunications, payment systems, and AI models means disruptions can ripple across a company and its customers. A single outage or policy change can affect multiple business lines if they are built on the same third-party stack. Knowing which third-party technologies underpin critical services is essential to continuity planning and disruption mitigation. That includes assessing where lock-in reduces flexibility, identifying realistic substitutes, and ensuring that data and processes can move between providers when needed, rather than being trapped in a single ecosystem.

Supply chains have also grown more fragile. Logistics bottlenecks, geographic concentration, and climate and energy transition risks have exposed single points of failure;. this reality has been further underscored by the pandemic. For example, the blockage of the Suez Canal in 2021 demonstrated how a single incident can significantly disrupt global trade routes, delaying shipments and affecting supply chains worldwide. Organisations should scrutinise their networks to identify and hedge vulnerabilities, often by diversifying suppliers and reassessing geographic exposure through practical contingency plans. This is not only about adding vendors; it is about understanding interdependencies: where multiple "alternatives" rely on the same sub-tier manufacturer or transport corridor and verifying that proposed workarounds can be executed at speed under real-world constraints.

Cyber threats compound these pressures. Software supply chain attacks, identity compromises, ransomware, and the convergence of operational technology and IT increase the likelihood and impact of incidents propagating through third parties. Cybersecurity due diligence must therefore extend to suppliers and partners, ensuring they maintain vigilant and comprehensive practices that protect interconnected systems. In practice, this means moving beyond paper assurances to clear expectations for prevention, detection, and response, and confirming that those expectations can be met in a coordinated way during an incident, including timely notification and defined recovery roles.

Layered over all of this is simple unpredictability. While tools such as the Geopolitical Risk Index (GPR) and other approaches offer trend awareness, they cannot capture the full spectrum of risk. In practice, these assessments resolve into two buckets: direct exposure you can mitigate within the company, and indirect exposure mediated by your third parties. The latter is often the larger share of geopolitical risk. Recent crises were rarely anticipated, underscoring the need for adaptable strategies and resilient systems capable of absorbing shocks from unforeseen events. This is because "unknown unknowns" cannot be fully modelled. Organisations benefit from building flexibility into their third-party arrangements, such as options to shift volumes, pause activities, or transition services when external conditions demand it, supported by contingency plans that are well understood and can be enacted without delay.

Regulatory landscape

Regulatory oversight is evolving quickly and affects core aspects of operations, from data privacy and environmental standards to anti-corruption practices. A defining feature of these regulations is the shift in responsibility and liability. Oversight of vendors and intermediaries is no longer a matter of best practice but a legal requirement. Companies must embed supplier accountability into governance, contracts, and operational processes to remain compliant. Understanding third-party compliance obligations is, therefore, critical.

The following overview non-exhaustively captures the main regulations reshaping supplier oversight today. Under the DORA, financial institutions must embed oversight of ICT third-party dependencies into governance and contracts, including audit rights, termination clauses, and resilience testing with critical third-party providers. The DSA imposes trader traceability, compelling platforms to verify the identity of traders. This embeds due diligence obligations into supplier and partner onboarding processes. The NIS2 Directive requires essential and important entities, on a risk-based basis, to extend cybersecurity risk management to their supply chains, mandating assessments and controls for vendor resilience. The AI Act pushes compliance upstream and downstream: organisations will need stronger vendor diligence, contract flow-downs, technical traceability, and monitoring. The Data Act reshapes contractual practice, by requiring providers of data processing services to facilitate data portability and switching rights, reducing vendor lock-in and strengthening user autonomy. In practice, knowing and managing third-party risk is now both a regulatory requirement and a decisive factor in sustaining operational resilience amid geopolitical, cyber, and supply chain pressures. Annex I provides an overview of how evolving EU regulations translate into practical TPRM actions to strengthen resilience across ecosystems.

Against this backdrop, many organisations still struggle to operationalise TPRM at scale. The next section of this paper explores the most common failure modes and their root causes.

The challenge landscape: why current TPRM often falls short

In the modern corporate landscape, third-party relationships are indispensable for achieving business objectives. Yet, managing the plethora of risks associated with these external entities presents an intricate web of challenges.

Fragmentation of Data and Processes

As explored earlier in this paper, without shared ownership the picture fragments; here’s how that manifests operationally. Engaging with third parties traditionally spans multiple disciplines within an organisation. For instance, Legal departments assess contract risks; Procurement evaluates pricing; and IT manages data requirements. Each department operates within its silo, possessing only a small piece of the overall picture. This fragmentation often leads to a limited view of third-party risks, dispersed across various departments without a centralised point of oversight. No one in the organisation has a complete view of their third parties.

More short-sighted still is the lack of clear ownership of these fragmented challenges. The absence of a single problem owner means the issue is dissipated across stakeholders, seemingly invisible and unacknowledged. Yet, this invisibility impedes the organisation's ability to leverage third-party data for tactical and strategic decision-making.

In the context of the rapidly evolving regulatory landscape, it is crucial to understand the legal implications of fragmented processes. Fragmented management of supplier data, contracts, and processes exposes organisations to direct legal risk. EU regulations now assume that companies exercise continuous oversight of their third parties. If procurement, legal, and risk functions work in silos, obligations may be inconsistently applied leading to missed reporting, unenforceable contracts, or unmonitored subcontractors. For example, a cloud provider may meet one regulatory requirement but fail another, leaving the regulated entity legally accountable for the gap. Boards and executives are now exposed to such failures. For instance, under new frameworks, accountability extends explicitly to governance of third-party dependencies. The legal consequences may be significant including supervisory scrutiny, penalties, reputational harm, and even personal liability.

Fragmentation therefore extends beyond operational inefficiency to a potential legal liability. In a regulatory environment where third-party compliance is inseparable from company compliance, organisations must now also harmonise data, processes, and oversight mechanisms across the supplier's lifecycle.

Case Study: Anonymised Example

Consider a major multinational corporation where third-party data is disjointed across different systems and tools. Lacking effective linkages, the organisation grapples with coordination inefficiencies. Business Contract Owners (BCOs), for instance, are hesitant to engage with compliance-related tasks when these fall outside their traditional scope of duties. The resultant communication gaps foster a fragmented, siloed approach to TPRM, exacerbated by variations in Third-party Risk Management knowledge and clarity within and outside the organisation. Consequently, deliverables vary in quality, impacting the efficacy of contractual data.

Internal and External Pressures

Compounding the problem of fragmentation are external pressures, particularly regulatory requirements that are often misaligned or out of sync. This misalignment in scope, timelines and requirements in regulations becomes especially problematic in supplier oversight, where one event can trigger conflicting duties. For instance, a significant incident involving a third-party vendor may require immediate reporting under one regulation and delayed reporting under another, forcing organisations into duplicative or create inconsistent processes. Similarly, contract requirements can vary across regulations resulting in overlap and possibly conflict. For instance one law mandates audit rights for ICT providers, another prescribes data portability clauses, and another requires monitoring of AI vendors (each on different cycles). These overlaps are rarely harmonised during drafting, and only after regulations take effect do companies discover how the obligations conflict in practice. Organisations are not only required to comply with new regulations that, as described above, redefine compliance expectations; they must also continue to meet existing mandates and regulatory obligations. This is a challenge that has manifested in practice: the entry into force of GDPR in May 2018 compelled controllers across the EU to renegotiate extensive portfolios of data processing agreements. Two years later, Schrems II, judgment suddenly invalidated the EU–US Privacy Shield, thereby rendering that transfer mechanism unusable and obliging controllers dependent on U.S. service providers to adopt alternative safeguards, such as Standard Contractual Clauses supplemented with additional protective measures. Both developments highlight that evolution of regulatory standards consistently places Third-party Risk Management under legal and operational stress, and entities that rely on reactive adjustments rather than resilient, forward-looking compliance frameworks incur the greatest exposure to disruption.

Corporations find themselves embroiled in several and separate inventories, assessments, and contract remediations that do not align. Disconnected tools like Procurement, Contract Lifecycle Management (CLM), Governance, Risk, and Compliance (GRC), and Configuration Management Database (CMDB) further contribute to inefficiency due to inconsistent identifiers and data silos. In multinational entities, uncertainties regarding data residency and cross-border transfers add another layer of complexity.

Common Pitfalls

While effectively managing third-party risk is paramount, organisations often encounter several recurrent pitfalls that hinder their strategies:

- Excessive Reliance on Static Assessments: Many organisations depend heavily on traditional questionnaires for third-party evaluation. This method, while straightforward, fails to capture the dynamic nature of risk, thus underscoring the necessity for continuous and real-time monitoring mechanisms.
- Uniform Control Measures: The adoption of a one-size-fits-all approach to controls can stifle operational flexibility. Such standardised measures often lack the necessary proportionality to accommodate the varying levels of risk associated with different third-party engagements, leading to inefficiencies and slowed business processes.
- Overlooking Fourth Party Risks: The exposures associated with fourth party interactions and beneficial ownership are frequently neglected. This oversight can result in significant blind spots within risk management frameworks, leaving organisations vulnerable to indirect risks they have not adequately assessed or mitigated. Furthermore, fourth party insight is likely to become the future norm in branches of risk management and compliance, such as cyber, sanctions, and supply chains.
- Premature Tool Implementation: Driven by the allure of technological solutions, some organisations prioritise tool acquisition without establishing a robust underlying operating model or data infrastructure. This premature focus can result in fragmented solutions that are misaligned with broader strategic objectives.
- Inadequate Contingency Planning: As discussed earlier in this paper, many firms lack properly tested exit, contingency or transition plans for their critical dependencies. The absence of contingency strategies can lead to significant operational disruptions in the face of sudden third-party failures or disengagements, and is conducive to geopolitical risk
- Misaligned Metrics and Risk Appetite: Finally, the disconnect between risk management efforts and organisational objectives often manifests in weak board-level metrics. When key performance indicators are not explicitly linked to risk appetite or strategic outcomes, it becomes challenging to gauge the true effectiveness of risk management initiatives and to communicate their value across the organisation.

Addressing these common pitfalls necessitates a more aligned and informed approach, integrating diverse organisational insights into a cohesive TPRM strategy that is both proactive and adaptable.

To overcome these failure modes, we turn to the fundamentals: a practical framework for good TPRM that establishes clear ownership, reliable data, and risk-based oversight as the bedrock for resilience.

Good TPRM: Building a Strong Foundation

In this increasingly complex and interconnected business environment, the need for robust Third-party Risk Management (TPRM) is more critical than ever. Implementations differ across organisations, but guiding principles can help shape strategic, tactical, and operational decisions. These principles serve as a benchmark for what constitutes good and great TPRM, allowing organisations to navigate risks effectively while maximising opportunities.

Core principles

Effective TPRM is anchored in a risk-based and proportional approach, moving beyond point-in-time assessments to continuous monitoring. By focusing on outcomes and dependencies, organisations can determine the right level of oversight for each relationship based on its criticality and potential impact on the business. Good TPRM is not siloed; it is integrated with procurement and linked to the organisation's broader strategy, risk appetite, Company Risk Management (ERM), cyber resilience, and governance structures. This holistic approach ensures TPRM is not an isolated function but a strategic component of the operating model, with clear governance, roles, responsibilities, and metrics for measurement. Critical (service) suppliers can be defined through their relation to critical processes within an organisation, allowing for quick mapping where potential weaknesses are formed or amplified by third parties. Within this construct, organisations should employ a tiering and criticality model that aligns with their risk appetite and regulatory frameworks. Such a model allows clear categorisation of third-party relationships, ensuring resources are allocated efficiently and effectively to areas of highest risk.

Data, tooling, and operating model

A strong data and tooling foundation underpins effective TPRM. Utilising a single source of truth is crucial. By integrating procurement and Contract Lifecycle Management (CLM) data, and using persistent identifiers such as the Legal Entity Identifier (LEI), organisations can achieve accurate entity resolution, improve data quality, and reduce the risks associated with fragmented information. While tools are essential in supporting TPRM efforts, they should not lead the process. Advanced technologies like AI can assist in triaging, summarising, and extracting clauses from contracts, but maintaining human oversight ensures judgment and context are not lost. For example, AI might efficiently scan vast contracts for specific risk clauses, while expert review adds a necessary layer of validation and strategic insight. Integrating external data feeds into TPRM tooling, such as sanctions lists, adverse media, cybersecurity posture scores, financial health indicators, and geolocation or country risk data further enriches the organisation's ability to assess and monitor risks dynamically.

AI tool: PwC's AI tools, LeAh and CREANCE.AI, are designed to transform legal and compliance workflows, with a broad application scope extending beyond DORA to encompass various aspects of regulatory risk management. LeAh automates tasks such as risk identification, contract redlining, and drafting of legal documents, leveraging deep engineering, multilingual ingestion, and embedded legal expertise. Additionally, LeAh offers advanced capabilities to compare agreements against policies, ensuring accurate transposition and highlighting any gaps. CREANCE.AI complements this by offering secure, high-quality contract analysis with full data anonymisation, encrypted exchange, and flexible deployment options, including SaaS and PwC-managed services. Both platforms support scalable, compliant operations and ensure consistent quality across jurisdictions. Together, they exemplify PwC's commitment to embedding AI into regulatory processes with precision, security, and operational efficiency.

Operating model choices determine how consistently these principles translate into action. Organisations should centralise expertise in TPRM, combining compliance and business intelligence to set standards, while enabling federated execution across business units to ensure cohesion and alignment in day-to-day activities. Integrating TPRM with operational resilience and cybersecurity further strengthens organisational defences. Comprehensive service-to-vendor mapping brings this to life by tracing dependencies from services to vendors, activating all involved stakeholders and promoting a collaborative approach to risk management.

A good TPRM strategy also involves risk-based monitoring: scale pre-contract due diligence according to supplier criticality, conduct ongoing monitoring for critical suppliers, and use point-in-time checks for less critical ones.

Great TPRM: Going Beyond the Basics

Great TPRM enables organisations to transcend traditional limitations and potentially capitalise on possibly risky but rewarding opportunities. By lowering the barriers to collaboration with higher-risk third parties through robust risk management processes, organisations can unlock new value streams that might otherwise remain inaccessible.
Additionally, effective TPRM can improve scenario planning by providing the organisation with greater insight into its third parties, allowing this information to be considered when developing scenarios.

Furthermore, great TPRM allows organisations to monetise the value generated by their risk management activities. By demonstrating how these efforts enhance strategic positioning, reduce costs, or enable new revenue opportunities, organisations can turn risk management into a competitive advantage.

Finally, great TPRM means having the insight in a company's third parties to such a degree that the exterior, surrounding ecosystem can be taken into consideration when orienting on strategy and playing out various scenarios on risks and opportunities. By assessing the qualities of suppliers, IT services, and so on, companies can enable a broad-spectrum view of plans and potential shifts.

In summary, by adhering to these principles, organisations can elevate their TPRM frameworks from good to great, strengthening not only compliance and risk mitigation but also strategic value creation and long-term resilience.

A couple of solution directions for parties looking to begin their journey

In embarking on the development and enhancement of TPRM frameworks, organisations have the opportunity to not only safeguard compliance but also protect and uncover strategic value. This chapter outlines practical steps and strategic considerations for companies seeking to establish or refine their TPRM processes, offering a pathway to robust, resilient partnerships. While these steps may not be exhaustive or sequential, they serve as a valuable guide for navigating the complexities of Third-party Risk Management.

Inventorying Essentials: Aligning Regulatory Requirements and Strategic Objectives

The first step in any TPRM initiative is to establish a clear inventory of regulatory requirements specific to your industry and geographical operations. Conducting a short study on missed potential allows organisations to visualise how current processes might fall short of unlocking strategic opportunities. Regulatory horizon scanning tools are increasingly used to assist in this study. By linking these potential areas to the company's overarching strategic objectives, firms can align compliance efforts with broader business goals, ensuring that risk management serves a dual purpose of safeguarding operations and driving success.

Practical Implementation: Engage Stakeholders and Define Short-term Actions

Taking immediate action requires both clarity and collaboration. Before diving into implementation, start with a comprehensive inventory of all third parties involved, not limiting the view to direct contracting partners but extending oversight to the entire supply chain. This process is crucial for understanding interdependencies, as your third-party may heavily rely on another entity within the chain. Once this inventory provides a clear picture of the interconnected landscape, your next immediate action requires clarity and collaboration.

Identify stakeholders impacted by third-party risks and bring them together to discuss practical implementation methods. Start by pinpointing critical suppliers requiring contract remediation, mapping their relations to critical processes, appointing accountable owners, potentially linking process and supplier ownership, and defining supplementary processes for organising the required remediations, including necessary inputs and timelines. This collaborative approach not only ensures buy-in but also fosters shared responsibility and transparency across the organisation.

Case Study:

A leading multinational consumer goods organisation faced the challenge of formalising its TPRM program and complying with the NIS2. A decentralised approach was taken to assess and onboard Information & Communication Technology (ICT) third parties through a manual process. This resulted in a lack of governance, limited formalised processes and no auditable trail across the procurement life cycle.

PwC supported the client in formalising the ICT TPRM process through the development of an ICT TPRM framework that outlines the requirements and governance across the different stages of the life cycle. This was supported by the development of an inherent risk questionnaire, due diligence questionnaire, and development of workflows to classify and assess third parties based on their criticality. Furthermore, PwC supported the client in setting up a centralised solution (client GRC system), assisted with the automated workflows and implemented security principles to minimise manual intervention and reporting.

Streamlining Onboarding Processes: Identifying and Rectifying Inefficiencies

Organisations must critically evaluate current onboarding and maintenance processes for third-party relationships. Identifying inefficiencies allows them to decide upon optimal adjustments and redefining roles and responsibilities to best fit the company's structure and culture.

Case Study:

A leading multinational organisation partnered with PwC NL to address inefficiencies in its third-party onboarding and maintenance processes. The existing system was fragmented, with limited visibility into supplier operations and inconsistent risk data integration. PwC implemented a comprehensive TPRM operating model that unified people, processes, and technology across the onboarding lifecycle. Using tools such as multi-domain questionnaires, AI-driven adverse media scanning, and integrated sanctions databases, the organisation was able to identify bottlenecks, redefine roles and responsibilities, and recalibrate third party engagements to align with its structure and culture. This transformation not only enhanced supply chain resilience but also ensured regulatory compliance and improved risk transparency across the vendor portfolio.

Building a Business Case for Strategic Value Protection

Each organisation must build a tailored business case highlighting missed strategic value and protection beyond compliance. This involves mobilising key roles, such as an executive sponsor, a TPRM lead, procurement and cyber resilience leaders, legal and CLM experts, and, finally, data architects. By engaging these stakeholders, organisations can ensure a comprehensive approach that considers every facet of third-party risk and strategic alignment.

Translating Strategy into Risk Reality

The success of TPRM relies on a cohesive translation of strategic decisions into actionable risk management practices. This involves:

- **Agreeing on Risk Appetite:** Define the acceptable levels of risk, particularly concerning ecosystem interdependencies, to guide strategic engagements with third parties.
- **Defining Critical Services/Suppliers:** Establish criteria to identify critical suppliers and prevent overburdening organisational resources while ensuring adequate risk management.
- **Connecting suppliers to processes:** Link the organisation's operating model and critical processes to the required ecosystem and integrate with existing structures of risk and process ownership.
- **Operationalising Concentration Risk Limits:** Implement strategies to manage concentration risks, balancing dependency and diversity across suppliers.
- **Board Reporting and Continuous Improvement:** Establish regular reporting cycles to the board, integrating learning loops for continuous improvement based on insights from TPRM activities.

These decisions should be routinely evaluated and refined through feedback loops, facilitating adaptive responsiveness to emerging risks and opportunities.

Embedding and Automating TPRM

Borrowing insights from financial crime prevention, organisations can embed TPRM within product lifecycles, ensuring risk management is inherent to business processes. Continuous supplier resilience testing and monitoring, risk-based in nature, enhances predictive capabilities.

DMS (Digital Managed Services) AI tool: Building on the integration of TPRM into product lifecycles, a global industrial manufacturer implemented PwC's AI-driven platform to embed risk management directly into its supplier onboarding and monitoring processes. Using modules like the Screener for sanctions and adverse media checks and the Outreach Portal for streamlined third-party communication, the company achieved real-time visibility into supplier risk profiles. The Reporter dashboard provided 24/7 access to operational insights, enabling proactive risk mitigation. This approach not only enhanced predictive capabilities but also ensured compliance and resilience across the supply chain.

Organisations should establish comprehensive sanctions and Ultimate Beneficial Ownership (UBO) screening processes for critical vendors. Developing a dynamic board dashboard offers transparency and allows for data-driven decision-making at strategic levels.

Managing Concentration Risks, Aggregation Risks and Strategic Diversification

Concentration risk management involves setting defined thresholds and strategically diversifying across regions and technology platforms, including leveraging multi-region and multi-cloud solutions. Regular failover testing ensures operational resilience and continuity.

Aggregation risk refers to the cumulative exposure an organisation faces when multiple third parties rely on the same underlying service providers, technologies, or geographic regions. Even when individual third parties appear diversified, hidden interdependencies, such as shared cloud infrastructure, subcontractors, or data centres, can create systemic vulnerabilities. Identifying and mapping these overlaps is essential to avoid single points of failure that could cascade across the supply chain. Effective aggregation risk management involves cross-functional data integration, dependency mapping, and scenario testing to uncover and mitigate these latent concentrations. Vice versa, if diversifying suppliers to curtail risks such as those stemming from geopolitical disruptions, TPRM becomes a necessary skill to manage and monitor that new source of resilience. Scenario planning (to practice responding to unforeseen events) can then be made more effective through the TPRM component, as the organisation will have better insight in its third parties, which can be taken into account when running scenarios.

Finally, developing comprehensive exit and transition plans for critical dependencies and conducting periodic resilience exercises with key vendors solidifies organisational preparedness against unforeseen disruptions.

Operationalising Efficiency

To bolster system efficiencies standardisation of key TPRM processes can reduce time spent on individual contractual parties. This can be achieved, for instance, through standard contract clauses for remediation, which can be deployed en masse, ensuring consistency and efficiency.

TPRM practices can integrate automated processes for beneficial ownership and sanctions screening, while maintaining detailed country-of-operation metadata. For globally active parties exposed to geopolitical risks, crafting a country risk model with defined triggers and engaging in scenario planning can mitigate sudden disruptions from sanctions, trade restrictions, or regional conflicts.

Geopolitical risk assessment AI tool: PwC's Geopolitical Risk Assessment tool enables organisations to rapidly benchmark their internal control frameworks against material geopolitical risks, using a structured "Quickscan" approach. By mapping risks related to geopolitics, such as sanctions, regulatory changes, market volatility, and cybersecurity against the company's business model, strategy, geographic spread, and existing controls, the tool highlights gaps and maturity levels in real time.

This targeted assessment supports efficient prioritisation of remediation actions and crisis planning, ensuring that TPRM processes remain agile and responsive to evolving geopolitical threats. The tool's indicators can be adjusted to focus more on external or internal company risks and can point out key risks that are outside of a company's sphere of influence. As a result, organisations can streamline risk management and enhance resilience across their third-party ecosystem accordingly.

By implementing these solution directions, organisations can build a resilient and agile TPRM framework that not only complies with regulatory demands but actively contributes to strategic success and competitive advantage in an unpredictable world.

Conclusion

As organisations navigate the complexities of modern business landscapes, the imperative to elevate Third-Party Risk Management (TPRM) from a mere compliance activity to a cornerstone of strategic resilience becomes paramount. This transition enhances the organisation's ability to proactively manage risks and leverage third-party relationships as significant drivers of value and competitive advantage. Additionally, it is becoming crucial to deal with geopolitical risks and anticipate disruptions originating outside of your sphere of influence.

Board-level visibility and measurable outcomes must define TPRM efforts. Tested playbooks and transparent metrics ensure that every initiative is scrutinised for efficacy, aligning risk management processes directly with business objectives. By establishing a clear view from the top, organisations can create a culture of accountability and foresight in managing external dependencies.

The journey toward robust TPRM starts small but with intent and purpose. Focusing on critical services, concentration hotspots, and conducting scenario tests are practical steps that yield immediate insights and operational improvements. These initiatives set a foundation for scaling efforts across the company and adapting to evolving challenges.

Further to these points, it is vital to embrace moments of crisis or missed opportunities as catalysts for change. Whether faced with a looming regulatory deadline or a failed cooperation due to process inefficiencies, these events should be harnessed as triggers for transformation. Avoid over-engineering (gold plating) what needs to be implemented, and instead use these disruptions as opportunities to streamline, sharpen focus, and refine processes.

The strategic case for comprehensive TPRM is clear: act now to foster resilience and unlock potential within third-party ecosystems. Organisations that embed strategic risk management in their core operations will not only comply with regulations but also position themselves for sustained growth in a complex and volatile world.

Authors

Netherlands

Casper Ruizendaal
Partner | Risk Consulting
casper.Ruizendaal@pwc.com

Lean Besseling
Director | Risk Consulting
lean.besseling@pwc.com

Jan Anthonie Hengst
Manager | Risk Consulting
jan.anthonie.hengst@pwc.com

Basmah Zaidi
Senior Associate | Risk Management
basmah.zaidi@pwc.com

Ilse van Wendel de Joode
Director | Digital Law & Commercial Contracting
ilse.van.wendel.de.joode@pwc.com

Marco Valkenburg
Senior Manager | Risk Consulting
marco.Valkenburg@pwc.com

Caitlin Verhoeven
Senior Associate | Risk Consulting
caitlin.Verhoeven@pwc.com

Annex I — EU digital decade: Practical third-party risk actions*

Regulatory pillar	Key focus	Third-party impact	Practical TPRM actions
Cyber & Resilience (NIS2, DORA)	Increase overall cyber resilience, with strict requirements for ICT risk, incidents, testing, and outsourcing	Vendors and ICT providers fall under direct scrutiny; focus on mandatory controls, contract remediation, earlier incident notifications, ongoing monitoring	Third-party inventory, embedding supplier security criteria in procurement, risk management measures, operational resilience testing, and contract remediation
Data & Privacy (Data Act)	Data protection, transfer of data, sharing/portability	Identify, manage and control third-parties that receive or provide access to data	Implementation of data sharing governance. Protecting confidential information and trade secrets. Setting up data access safeguards and controls. Update contracts by for example including data use restrictions, portability rights and termination rights
Data & Privacy (GDPR)	Data protection	Identify, manage and control third-parties that receive or provide access to data	Vendor due diligence, data processing agreements, conducting DPIA's and transfer assessments, ongoing monitoring and incident management
Platforms & Fairness (DSA, DMA)	Create safer online space, protect fundamental user rights, and establish a level playing field for businesses	Platform governance and accountability: selection of-contracts with-, monitoring of- ,and audit of third-party service providers	Third-party seller onboarding, verification and monitoring. Implementing en supervising notice and takedown mechanisms. Implementing third-party risk assessments and transparency obligations. Safeguard data interoperability, portability and non-discriminatory access
AI & Emerging Tech (AI Act)	Risk-based rules for developers and deployers regarding the use of AI	Classification of systems, verifications of third-party compliance, and embedding contractual measures	Conduct role and risk qualification of third parties. Require conformity assessment documentation; monitor/audit ongoing compliance and include contractual controls.
Product (Product Liability Directive (PLD))	Updated product liability standards to align with new technology, circular standards, and globalized supply chains	Liability extends beyond traditional manufacturers (supply chain contribution).	Strengthen due diligence, contracts, monitoring, and incident response with suppliers (especially for digital components), to prevent defects and defend claims. Focus on traceability, documentation readiness, and back-to-back obligations

Note:
*This overview is provided for general guidance and is not intended to be exhaustive.

Thank you