



Renewed Urgency on Third Party Risk Management (TPRM)



Evolving Business Climate

The overall business climate worldwide continues to be increasingly complex. Since the Covid-19 pandemic, we experienced an economic downturn, disruption in supply chains (raw material shortages, increased costs of production, transportation challenges) and volatility in capital markets. Not to mention ongoing regional conflicts, rising geopolitical tensions and trade wars.

As all of this happens, there are evolving risks faced across the board by organizations beyond the traditional or “known” ones (financial, compliance, operational, reputational). Companies are being reactive to ESG and cyber risks and compliance managers are constantly scratching their heads on how to manage the ongoing burden of regulation, while increasing stakeholder and shareholder value.

Business Reputation Human Rights and ethical labor

SUPPLY CHAIN DUE DILIGENCE Money Laundering Beneficial ownership

ESG Trade sanctions Bribery and corruption Ethical/sustainable Sourcing

Political exposure Fraud Data privacy and data security

You Cannot Outsource The Risk

Businesses across every industry are increasingly dependent on a robust network of third parties in order to execute their core activities. Such third parties include vendors, suppliers, distributors, agents, joint ventures, alliances, subcontractors, and service providers. This network is critical to maintain a global footprint and effectively compete in the marketplace.

The increased shift toward third-party driven business models, exposes organizations to a host of new and serious risk and compliance issues.

Additionally, as guided by various regulators and as many companies have experienced first hand, while you may trust the third parties you work with, the risks associated with third party interactions **cannot be outsourced**.

There are numerous cases where lack of proper oversight of third parties has resulted in serious consequences. Companies in the U.S. and globally have been exposed to significant risk, adversely affecting their performance and reputation, and have faced heavy enforcement actions resulting in heavy fines, penalties and remediation costs.

Common Third Party Risks

Some third party risks faced by organizations are outlined below:

Potential areas of third-party risks

Reputational risk

- Negative news
- Lawsuits
- Brand of the third party
- Key principals/owners of the third party
- Workplace safety
- ESG

Subcontractor risk

- Applicable across all risk areas

Strategic risk

- Service delivery risk
- Expansion/roll-out risk
- Mergers and acquisitions
- Alignment to outsourcing strategy
- Intellectual property risk

Operational/supply chain risk

- Business continuity
- Disaster recovery
- Physical security
- Operational resilience
- Performance management (incl. SLAs)
- Human resources risks

Concentration risk

- Supplier concentration across critical services
- Industry concentration (incl. subcontractor)
- Concentration of critical skills (i.e., tech support)
- Geographic concentration
- Reverse concentration

Regulatory/compliance risk

- Regulatory requirements
- Theft/Crime/Dispute risk
- Fraud, anti-bribery and corruption/sanctions
- Compliance with internal procedures and standards

Information Security & Technology Risk

- Technology
- Cybersecurity
- Privacy
- Artificial Intelligence Oversight

Country risk

- Geopolitical risk
- Climate sustainability

Financial viability

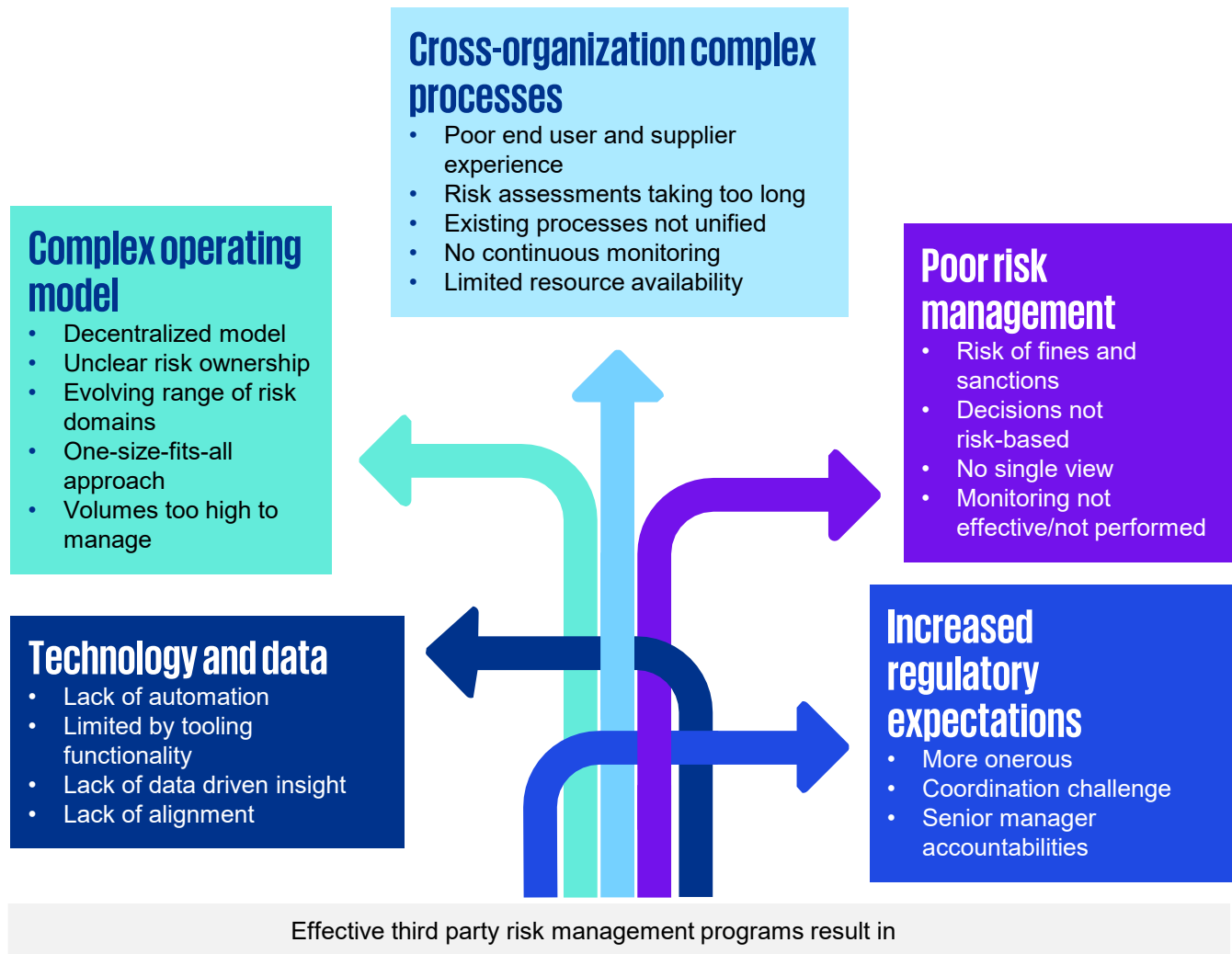
- Financial risk from lending to a third party
- Liquidity risk

Legal risk

- Jurisdiction of law
- Terms and conditions of the contract

A fundamental question to ask considering all of the above is **“Is your business protected when you bring in third parties to your network?”** For many organizations, allocating the resources, time, and effort for this critical task can be daunting.

Common challenges in managing third-party risk



While there are no immediate signs of any of these challenges letting up soon, it is still imperative for organizations to continue being resilient and proactive on their TPRM programs.



Our recent publication on Ten Key Regulatory Challenges of 2024¹ highlights how there is likely to be increased overall regulatory oversight which would result in ‘expectations for robust (and demonstrable) risk accountability’ and also proving sustainable risk processes including in areas such as risk quantification and integration. An interesting point arose around “threat actors” where there is likely to be expanding regulatory expectations around the detection, mitigation, tracking and remediation of perpetrators of financial crime, fraud, and misconduct.



KPMG’s 2022 TPRM Survey² called out how 77 percent of businesses struggle to maintain a fit-for-purpose TPRM operating model.



¹[ten-key-regulatory-challenges-of-2024.pdf \(kpmg.com\)](#)
²[Third-Party Risk Management Outlook 2022](#)

No Time To Be Complacent – Evolving Your TPRM Program

Good practice TPRM should be holistic and consider the following:

- Managing program requirements throughout the lifecycle of the relationship, from initiation to termination, including reporting to management.
- Risk-based program requirements, focusing time and effort on managing third parties that pose the greatest risks to their organization.
- Clear roles and responsibilities across three lines of defense to promote agility, point to emerging risks, and help clarify an organization’s strengths and weaknesses
- Fit for purpose technology and automation – the thinking beyond simply GRC platforms in order to use smarter technology for automating workflows, risk assessments and use of AI (such as agents/prompts) to streamline the process and shorten cycle times, enabling companies to concentrate on their core activities.

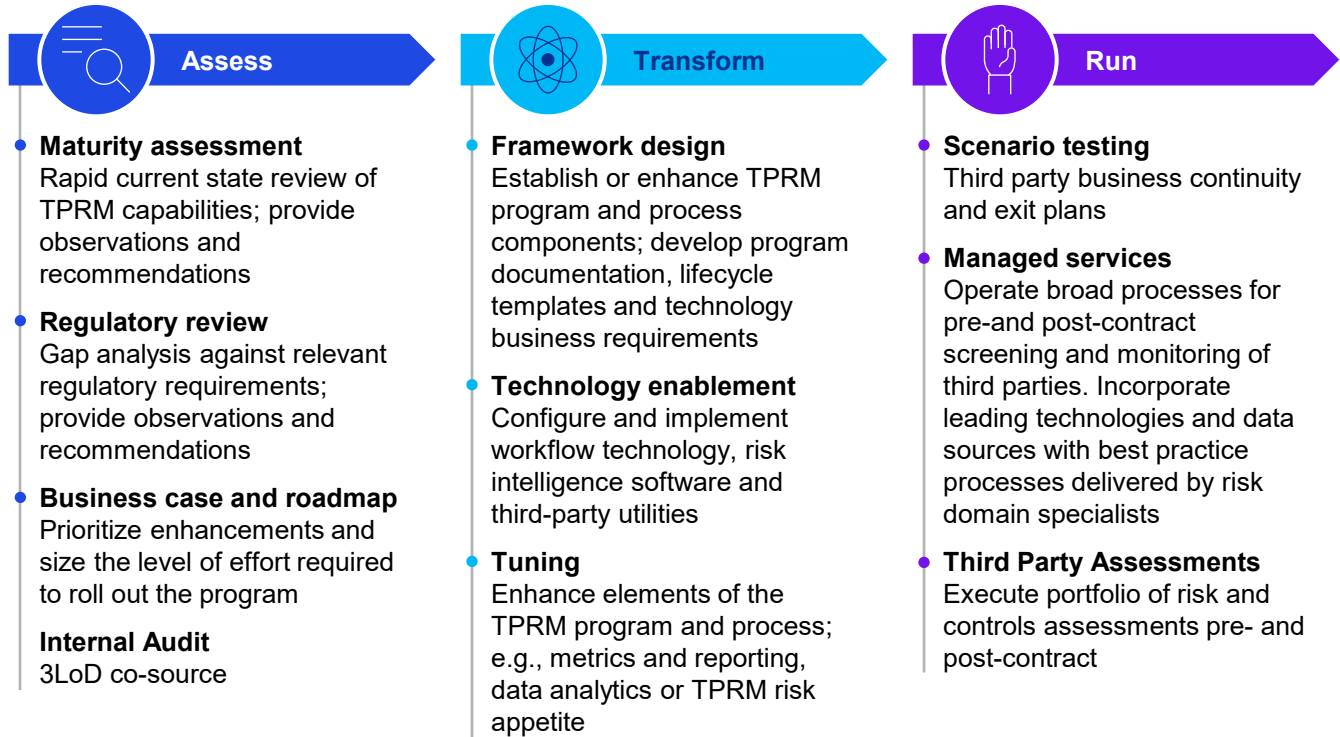
The KPMG view of the elements that constitute an effective TPRM program is set out in the graphic below.



How Can KPMG Assist You

We bring to the table a network of TPRM professionals with deep subject-matter experience to help deliver TPRM program designs for clients' global operations and regulatory requirements. Our professionals possess **cross-industry experience across all industry sectors** and leverage leading technology solutions and delivery experience through **established TPRM methods and technology accelerators**.

How we help clients



Outcomes

- Strong, compliant and consistent framework across the enterprise
- Intelligent risk scoring model
- Risk-based and robust screening, due diligence and monitoring
- Automation of inherent risk assessment and due diligence activities
- Reduced onboarding cycle times and program costs with optimized and streamlined processes
- Real-time monitoring and alerting to anticipate service disruptions before they occur
- Insights and analysis to track, report and predict
- Integration with complementary processes and tools (procurement and contract lifecycle management)

Solutions and services

Service category and objectives

Vision and program design

- Assess TPRM activities against applicable global regulatory requirements and industry leading practices
- Define the vision and strategy of the TPRM program by designing a target operating model

Implementation and enhancement

- Design, build, implement, and assess TPRM specific requirements for risk areas as well as functional technology requirements
- Streamline and/or remediate pain points in the program to help enhance efficiency and effectiveness

Operational execution

- Solve challenges related to lack of skilled staff to execute the day to day TPRM activities.
- Drive the value of TPRM program by providing transparency to third party risk and performance

Key services

TPRM program

- **Program Design:** target operating model and service delivery model development
 - Gap assessments against global TPRM requirements
 - Development of these models at the 2nd LOD, 1st LOD and regional operating levels
- **Program documentation:** policy, procedures and standards development
- **Global TPRM services:** Assist with compliance with local regulations

TPRM services

- **Integrity due diligence:** reputational assessments through research of adverse news/litigation/ownership
- **Cyber TPRM reviews:** conducting cyber risk assessments and due diligence reviews on an ongoing basis as a managed service

TPRM risk programs

- **Compliance TPRM:** program design, compliance TPRM risk assessments and due diligence questionnaires, regulatory consumer compliance mapping to contracts for risk assessment and testing
- **Cyber TPRM:** program risk assessment, CISO cyber TPRM program design, risk segmentation
- **Fourth Party/Subcontractor Risk Management:** program design, inventory development
- **Operational Resiliency:** integrating TPRM program in operational resiliency planning
- **Convergence experience:** aligning risk assessments to reduce duplication and drive cost savings

Contract management

- **Cognitive Contract Management:** using AI/NLP to collect and analyze contracts
- **Contract Performance Management:** managing critical contracts SLAs to avoid value leakage
- **Contract Compliance:** avoidance of fines and penalties or assessing compliance with you contract terms at your customers
- **Exit Strategies:** development of and assessment of exit strategies

Technology enablement

- GRC/other TPRM technology implementation: Assist with scoping of right-sized technology requirements
- Strategic partnerships with GRC platforms/utilities as desired (example: ServiceNow, etc.)



Contact Us



Daniel W. Click
Partner, TPRM
KPMG LLP
T: 220-219-3521
E: dclick@kpmg.com



Joseph P Gyengo
Principal, TPRM
KPMG LLP
T: 404-863-5801
E: jgyengo@kpmg.com



Jilane Khakhar
Director, TPRM
KPMG LLP
T: 212-954-1181
E: jilanekhakhar@kpmg.com



Lauren Polana
Director,
Forensic Services
T: 267-256-3209
E: lpolana@kpmg.com



Kyle Thompson
Director,
Forensic Services
T: 404-222-3441
E: kylemthompson@kpmg.com

Learn about us:



[kpmg.com](https://www.kpmg.com)

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

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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS041379

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.