A challenging new reality for Consumer & Retail businesses

Third-party risk is on the rise amid global challenges, supply chain disruption, and fraud

Retail and consumer goods businesses are at a critical crossroads in their management of third-party risk amid an alarming array of challenges that include COVID-19, unprecedented supply chain volatility, heightened regulatory scrutiny and the threat of fraud and corruption.

Today's global environment is nothing less than a new reality for these businesses, and we believe they have no time to lose in pursuing holistic third-party risk management (TPRM) programs that are designed to address the world of risk they now inhabit.

Consider the dramatic challenges and trends that are disrupting this sector, starting with COVID-19. The global challenge has unleashed profound new inventory challenges — many businesses facing a severe shortage of inventory while others grapple with oversupply and an inability to liquidate. Consumer goods manufacturers, meanwhile, are often chasing raw materials to meet demand.

In response, many companies are shifting supply chains to new geographies and accelerating their supplier onboarding process — often ignoring required TPRM controls and thereby heightening the risk of violations that can include third-party fraud, corruption and bribery. Some suppliers, meanwhile, are desperately engaging their own sub-contractors, 'fourth parties' to the companies themselves, without executing the due diligence, controls and monitoring required for these relationships. Some businesses are unfortunately discovering after the fact — if at all — that fourth-parties have even been enlisted.

The impact of COVID-19 is also driving a trend toward cost-cutting, and that can include less attention paid to necessary supplier audits and other ongoing monitoring of third parties. Authorities, meanwhile, are seeing a disturbing proliferation of counterfeit goods being marketed to cover chronic inventory shortages, plus a rise in bribery, fraud and corruption to facilitate faster exporting or importing of goods and raw materials to keep businesses moving.

Regulators are sharpening their focus

We are also witnessing in today's extreme environment a shift to 'economic nationalism,' as consumers continue to exhibit a preference for domestic or locally produced goods. Today's 'make where you sell, buy where you make' mindset is forcing many companies to quickly source appropriate new 'homegrown' suppliers — sometimes at a higher cost and often with less scrutiny or due diligence in the rush to remain competitive, if not viable.

Heightened regulatory scrutiny is also pressing down on the retail and consumer sector — which has traditionally faced less oversight compared to, say, banking and financial services. The spotlight on the sector — and the attendant risk of severe penalties — is growing more intense amid the unmistakable rise in General Data Protection Regulation (GDPR), human trafficking, economic sanctions, and other areas of regulatory focus.

Make no mistake — with supply chains in flux and the risk of significant fines, penalties and business interruption soaring, today's retail and consumer goods businesses are mired in a disturbing new reality that has them concerned about their future.

Third-party relationships are a significant source of competitiveness and growth for businesses operating in today's complex global markets. But without holistic, technology-enabled oversight programs that are closely aligned to meet today's fast-evolving risks, supply-chain relationships become a weak link that exposes businesses to an array of potentially catastrophic risks.

That's where TPRM comes in — understanding the organizational risks presented by third-parties, assessing whether they can effectively manage current and emerging risks as needed, and establishing consistent oversight and monitoring.

But as our global research shows, businesses still have considerable ground to cover on the journey to effective TPRM programs.

KPMG survey reveals a lack of progress on TPRM programs

KPMG 2020 global online survey of 1,100 senior TPRM executives, including consumer goods and retail-sector leaders, reveals that the journey to effective TPRM has, for many businesses, barely begun despite today's extreme challenges:

- Retail and consumer goods businesses cite business growth enablement, data governance/privacy, cost efficiency, cyber-risk management and brand reputation as 'business critical' initiatives. Yet half of these businesses lack in-house capabilities to manage all third-party risks faced, with TPRM funding described as limited (51 percent) or scarce (20 percent), and 63 percent of respondents say their TPRM teams are 'undervalued.'
- Retail and consumer goods organizations have various TPRM processes in place today: assessment of third-parties before contract (41 percent); third-party monitoring (36 percent) or on-site assessment (33 percent); a risk-based monitoring approach (35 percent); second-line (33 percent) or third-line (36 percent) oversight of TPRM and third-parties.
- Only about one in three organizations in these sectors say they are 'highly proficient' in areas such as global compliance; managing global third-party issues; managing or improving cyber defenses; collaborating with internal stakeholders/partners; and fully understanding third-party risk. Most instead view their abilities in these areas as merely 'adequate' or 'requiring improvement.'
- Respondents are challenged in their TPRM transformation efforts by the lack of necessary skills and capabilities (39 percent); integration challenges (30 percent); regulatory breach concerns (24 percent); employee resistance (35 percent); lack of funding (28 percent); data quality/consistency (27 percent).
- Sixty-nine percent of overall respondents viewed seamless data-sharing of third-party information as 'the holy grail of TPRM' – yet many experienced barriers to sharing third-party data, including incompatible systems, privacy concerns, inconsistent data, insufficient resources, and/or organizational silos.
- Regulatory scrutiny of third-party relationships and privacy breaches/loss of customer data is growing – 59 percent of respondents overall faced sanctions or regulatory findings related to TPRM. Six of 10 respondents say the highest reputational risks come from third parties' failure to deliver.

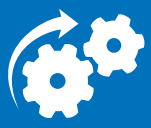
KPMG framework for success in a new era

As KPMG firms work with clients pursuing TPRM solutions for an unprecedented era of needs and challenges, we have developed one of the leading and tested frameworks for TPRM transformation built on four pillars: *Governance, Process, Infrastructure, Data.* Each has specific requirements, as illustrated ahead.

Governance

What is required?

- A single TPRM program leader.
- A reporting structure to senior management and the Board.
- An enterprise-wide outsourcing and third-party strategy and a defined risk appetite.
- Clear responsibilities and accountabilities across the TPRM program and lifecycle.
- Policies, standards and a risk appetite that establish the scope and focus of the program.
- An inventory of third-party services to which the program applies, with clearly defined services.



Process

What is required?

- Consistency of execution across the organization's business units to drive quality data for analysis and integration with the second and third lines of defense.
- Assessment teams possessing the right mix of skills, expertise and bandwidth.
- A risk-based approach to assessing third-party services, tied to the program's risk appetite.
- Risk assessment and due diligence prior to contract execution and decision making.

Infrastructure

What is required?

— TPRM technology architecture that supports efficient workflow, task automation and reporting across the entire business.

— A documented and well-understood audit trail.

— A service delivery model that's aligned to the company's operating style — centralized or distributed — that enables consistent management of risk across business lines and regions.

— Integration of TPRM activities and technology organization-wide into processes, such as procurement, legal and finance, and into existing risk-oversight functions and activities.

Data

What is required?

— Collection of real-time data around the TPRM program's ability to manage third-party assessments, onboarding, and monitoring, and the ability to manage the performance of each third-party service and their control environments.

— A comprehensive data model for collection of third-party information, including service details, risk scoring, contract information and performance monitoring.

— Internal data feeds that monitor and record specific events and incidents attributable to third parties, and external data feeds that monitor for real-time information on the third parties, such as adverse media, changes in business ownership, corporate actions, cyber vulnerability scores, and financial viability ratings.

— A process to update third-party risk profiles when there are changes to the risk score.

— Real-time tracking of performance against service level agreements (SLAs) and real-time tracking of risks against key risk indicators (KRIs).

— Data-driven decision making, where risk assessments and performance monitoring influence contracts and decisions.

There is no time to lose on the journey to TPRM maturity

Beyond TPRM transformation programs that are optimized across these four pillars, sustained success requires ongoing program uplifts, process optimization and innovation. Companies grappling with uncertainty and disruption can no longer ignore these key steps to progress:

Agree on the vision: A key consideration for an enterprise-wide TPRM program is designating program ownership and determining where TPRM sits within the organization.

Build the model: TPRM programs are complex, meaning development is not a one-time exercise but a work in progress requiring businesses to 'strike the right balance.'

Optimize the process: The program should include mechanisms to ensure that third parties failing to meet risk criteria and materiality thresholds are not put forward for assessment by the TPRM program.

Evolve and innovate: TPRM programs typically revolve around the gathering and assessment of third-party data. The future will demand rethinking on how data-driven, proactive risk monitoring via AI and machine learning will likely identify early-warning indicators for third-party resilience.

In conclusion, it's abundantly clear that today's retail and consumer businesses are being tested as never before. As our survey shows, it will be no easy task to close the gap between today's heightened risk environment and the ongoing lack of TPRM funding, resources, skills and initiatives. But the new reality dictates that timely, strategic change is critical to ensure future viability, growth and success, and businesses that delay the TPRM journey might do so at their own peril.

Contacts

Amanda Rigby
Principal
KPMG in the US
E: amandarigby@kpmg.com

Alexander Geschonneck
Partner
KPMG in Germany
E: ageschonneck@kpmg.com

Leah Jin
Partner
KPMG in the Netherlands
E: Jin.Leah@kpmg.nl

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

home.kpmg/socialmedia