Industrial manufacturers struggle on the road to third-party risk management maturity

Roadblocks include a lack of strategies, skills, technology and investment

Volatile global markets. Trade wars and protectionist tariffs. Reputational risk amid human-rights violations that include illegal labor and human trafficking. Regulatory scrutiny and potentially devastating penalties. The imposing threat of catastrophic cyber attacks.

These are historically turbulent times for the industrial manufacturing industry. And the profound impact of COVID-19 continues to heighten industry challenges as organizations endure supply-chain disruption, inventory volatility, cost cutting, and potential fraud and corrupt practices among suppliers.

Third-party relationships are increasingly embraced as a critical source of competitiveness and growth in today's remarkably challenging global environment. Yet, as our 2020 global survey of third-party risk management (TPRM) executives illustrates, industrial manufacturers are struggling to implement robust, sustainable TPRM programs amid the lack of strategies, investments, skills and technologies considered critical for the consistent selection, assessment and monitoring of third parties.

Without holistic, technology-enabled oversight programs, those relationships can become a weak link — exposing businesses to an array of significant risks that include reputation damage as well as operational and cost implications. That's where TPRM comes in — understanding the organizational risks presented by third parties, assessing whether they can effectively manage those risks, and establishing consistent third-party oversight and monitoring. A properly functioning TPRM program provides critical insights that include:

How the third party will access, store and transmit enterprise data;

Whether third parties maintain a control environment that meets the organization's needs;

Whether a third party will represent your organization to others, including government officials;

Which specific requirements need to be negotiated into third-party contracts.

But beware. A simple 'one-size-fits-all' TPRM program does not exist. Each requires an informed and precisely defined strategy that's supported by a well-defined risk appetite.

Throughout this document "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

© 2020 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Today's TPRM demands a holistic, risk-based approach

Our research reveals that for many manufacturers, the journey to TPRM maturity continues to face roadblocks. KPMG's 2020 global survey of 1,100 senior TPRM executives of businesses reporting annual revenue of US$200 million to more than US$20 billion included 184 global industrial manufacturing organizations. Among them, 71 reported annual revenue of US$200 million to US$1 billion, 46 had revenue of between US$1 billion and US$5 billion, and 67 had revenue exceeding US$5 billion.

As our findings illustrate, many of these organizations remain unprepared for the complexity of assessing diverse risks cohesively across business lines and global geographies. For many, the journey to effective TPRM has barely begun despite today's extreme challenges.

Holistic risk identification and assessment during onboarding and throughout the contract lifecycle is crucial to maintaining a line of sight into the risk profile of the entire third-party portfolio. Today's businesses need to take a *risk-based approach* to assessing and monitoring third parties that present the highest risk to the organization.

This is particularly true amid today's disruptive COVID-19 environment and KPMG has defined four phases for businesses to consider in response to the pandemic: Reaction, Resilience, Recovery, and the New Reality.

— **Reaction and Resilience:** Implementing emergency shifts to remote working models, and rapid reconfiguration of third-party service-delivery models;

— **Recovery and the New Reality:** Preparing for subsequent virus outbreaks, new government regulations and supplier uncertainty.

KPMG's framework for success in a new era

As KPMG professionals work with clients pursuing TPRM solutions for an unprecedented era of needs and challenges, we have developed a framework for TPRM transformation that's built on four pillars: *Governance, Process, Infrastructure* and *Data.* Each has specific requirements, as illustrated below.

Governance

— A senior leader responsible for the TPRM program;

— 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 program scope and focus;

— An inventory of well-defined third-party services to which the program applies.

Process

— Consistency of execution across the organization's business units to drive quality data for analysis and integration with second and third lines of defense;

— Assessment teams possessing the right mix of skills, expertise and bandwidth;

— A risk-based approach to assessing third parties, tied to the program's risk appetite;

— Risk assessment and due diligence prior to contract execution and decision making.

© 2020 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Infrastructure

— TPRM technology architecture that optimizes 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 — and that enables risk management across business lines and regions;

— Integration of TPRM organization-wide to enhance functions such as procurement, legal, finance, risk oversight and more.

Data

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

— A broad-ranging 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 third parties, such as adverse media, changes in business ownership, corporate actions, cyber vulnerability scores, financial viability ratings;

— A process to update third-party risk profiles resulting in 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.

KPMG survey: the TPRM journey has barely begun

As our research shows, many businesses within the manufacturing sector and beyond still lack the critical technology, funding and skills needed for effective TPRM programs:

Manufacturing businesses surveyed cite cyber-risk management, data governance/privacy, cost efficiency, business growth and brand reputation as 'business critical' initiatives. Yet 45 percent still lack the in-house capabilities needed to manage all third-party risks, with TPRM funding described as limited (51 percent) or scarce (21 percent), while 58 percent also believe their TPRM teams are 'undervalued.'

Manufacturing businesses have the following TPRM processes in place today: assessment of third parties before contract (44 percent); third-party monitoring (40 percent) or on-site assessment (35 percent); a risk-based monitoring approach (41 percent); second-line (36 percent) or third-line (37 percent) oversight of TPRM and third parties; regular reporting of TPRM to senior management (42 percent).

Three-quarters (74 percent) of overall respondents admit that their organizations 'urgently need to make TPRM more consistent across the enterprise.' Among manufacturers, relatively few are 'highly proficient' in: ensuring global regulatory compliance (35 percent); managing global third-party issues (35 percent); managing or improving cyber defenses (33 percent); collaborating with internal stakeholders/partners (32 percent); fully understanding third-party risk (30 percent). Most sector businesses instead view their abilities in these areas as merely 'adequate' or 'requiring improvement.'

Principle challenges to TPRM transformation cited among manufacturers include: lack of skills/capabilities (36 percent); integration challenges (35 percent); regulatory breach concerns (37 percent); employee resistance (26 percent); lack of funding (27 percent); data quality/consistency (3s0 percent).

Seamless data sharing of third-party information is viewed as 'the holy grail of TPRM' by 69 percent of overall respondents, yet many firms continue to face barriers to sharing third-party data: incompatible systems, privacy concerns, poor or inconsistent data, insufficient resources/processes, 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 concerning TPRM. Six of 10 say their highest reputational risk comes from the failure of third parties to deliver.

© 2020 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Overcoming roadblocks to TPRM maturity

Beyond TPRM programs that are optimized across these four pillars, sustained success toward maturity requires ongoing program uplifts, process optimization and innovation. Successful TPRM transformation demands strategies to overcome roadblocks that have plagued systems throughout their initial build and subsequent iterations. These include:

— Inadequate executive support and tone at the top;

— Resistance to organizational realignment;

— Large resource needs to operate the program;

— Insufficient accountability from third-party businesses;

— Lack of investment in technology enablement;

— Resistance from third parties to co-operate with the TPRM process.

Companies grappling with uncertainty and disruption can no longer ignore these key steps to TPRM maturity:

Agree on the vision: A key consideration for an enterprise-wide TPRM program is designating program ownership and establishing 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' over time.

Optimize the process: 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-part data. The future will demand rethinking on how data-driven, proactive risk monitoring via AI and machine learning will identify early-warning indicators for third-party resilience.

In conclusion, we see today's industrial manufacturing businesses being tested as perhaps never before amid the rapid changes and demands that are inundating them. Unfortunately, the journey toward TPRM transformation remains a slow-moving work in progress for most manufacturers amid the need for funding, technology, new skills and more. Our advice to businesses is that strategic change toward a holistic, risk-based approach is inevitable to enable future viability, growth and success. And businesses that delay the TPRM journey might do so at their own peril.

Contacts

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

Daniel Click
Managing Director
KPMG in the US
E: dclick@kpmg.com

Jilane Khakhar
Director
KPMG in the US
E: jilanekhakhar@kpmg.com

home.kpmg/socialmedia

Throughout this document "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

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.

© 2020 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit home.kpmg/governance.

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

Designed by Evalueserve.
Publication name: Industrial manufacturers struggle on the road to third-party risk management maturity
Publication number: 137302-G
Publication date: December 2020