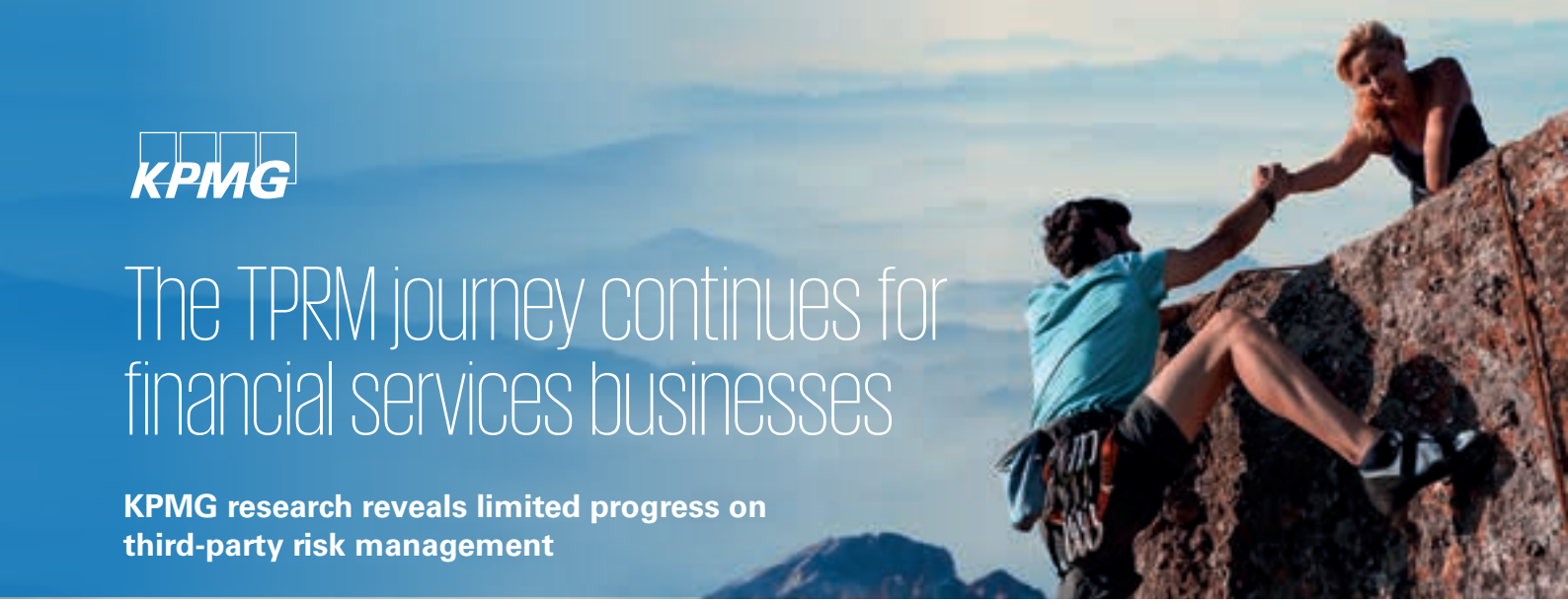

The TPRM journey continues for financial services businesses

KPMG research reveals limited progress on third-party risk management

In today's complex and volatile global markets, third-party relationships are a critical source of competitiveness and growth for financial services businesses. Financial institutions are increasingly reliant on third-party suppliers to deliver business-critical products and innovative services in the fast-paced and ever-evolving digital age.

But as our research indicates — and as the disruptive impact of COVID-19 has made clear — TPRM needs to be approached in a more-consistent manner that ideally relies on a centralized and refined service model across the entire organization. Failures by third-parties can rapidly tarnish business reputations, unleash significant downstream operational and cost implications, and generate significant penalties for regulatory non-compliance or misconduct.

While some financial institutions are indeed making progress on TPRM, particularly via technology innovation, many still need to invest in areas that include streamlining workflows and optimizing the technology enablement of their TPRM programs. Despite advances in governance, risk and compliance (GRC) solutions, many financial institutions today are still conducting many aspects of their TPRM process via email or spreadsheets.

Consider today's volatile environment a catalyst for improvement

Financial services (FS) businesses should view today's risk-laden environment as a tipping point toward heightened TPRM awareness, strategy and execution that ensures sustained and consistent third-party assessment, onboarding, oversight and monitoring. A properly functioning TPRM program provides critical insights that include:

— How the third party will access, store or transmit the FS organization's data;

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

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

No 'one-size-fits-all' TPRM program exists. Each requires an informed and precisely defined strategy that is supported by a clearly articulated risk appetite.

KPMG's global online survey of 1,100 senior TPRM executives of businesses reporting annual revenue of US$200 million to more than US$20 billion included 184 financial services organizations. Among them, 80 reported revenue of US$200 million to US$1 billion; 39 reported revenue between US$1 billion and US$5 billion; and 65 had revenue exceeding US$5 billion, including 13 with revenue above US$20 billion. And as our findings revealed, many of these organizations appear unprepared for the complexity of assessing diverse risks cohesively across business lines and regions.

Holistic risk identification and assessment during onboarding, and throughout the lifecycle of the contract, is crucial to maintaining a line of sight into the risk profile of the entire third-party portfolio. FS businesses need to take a *risk-based approach* to assessing and monitoring third-party products and services that present the highest risk to the organization. This is particularly true amid today's disruptive COVID-19 environment and on that front 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 moves to remote working models and rapid reconfiguration of third-party service delivery models;

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

Yet, as our research shows, many businesses within the financial sector and beyond still lack the critical technology and skills that underpin effective TPRM programs.

KPMG survey reveals weak progress on TPRM

— Six of 10 respondents overall cited third parties' failure to deliver as their highest reputational risk and have experienced sanctions or regulatory findings concerning TPRM. About three quarters overall called TPRM a strategic priority, saying they 'urgently need to make TPRM more consistent across the enterprise.' For FS organizations specifically, TPRM remains at the top of regulatory agendas globally and this trend is driving a focus on improving TPRM among sector businesses.

— Financial institutions cited cyber-risk management, data governance/privacy, cost efficiency, business growth and brand reputation as 'business critical' initiatives. But more than half lack in-house capabilities to manage third-party risk, with TPRM funding described as limited (48 percent) or scarce (30 percent). Meanwhile, 71 percent believe their TPRM teams are 'undervalued.'

— FS businesses have the following TPRM processes in place today: a total of 81 percent cited assessment of third parties before contract (38 percent) and third-party monitoring (43 percent); on-site assessment (29 percent); a risk-based monitoring approach (34 percent); second-line (32 percent) or third-line (38 percent) oversight of TPRM and third parties.

— Relatively few FS businesses believe they are 'highly proficient' in areas such as: managing global third-party issues (35 percent); managing or improving cyber defenses (39 percent); collaborating with internal stakeholders or partners (38 percent); fully understanding third-party risk (32 percent); ensuring global regulatory compliance (40 percent). Most view their abilities in these areas as merely 'adequate' or 'requiring improvement.'

— Key challenges to TPRM transformation cited among FS businesses include: Lack of skills (36 percent); integration challenges (30 percent); regulatory compliance concerns (34 percent); employee resistance (29 percent); lack of funding (30 percent); data quality/consistency (30 percent).

— Seamless data-sharing of third-party information is viewed as 'the holy grail of TPRM' by 69 percent of overall respondents but many firms face these barriers: incompatible systems, privacy concerns, poor or inconsistent data, insufficient resources or processes, and organizational silos.

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

While we see that the current focus in TPRM among financial institutions continues to center on program uplift and process optimization for cost and time savings, significant strides are being taken towards wholesale TPRM transformation. Leading TPRM programs are experimenting with innovative new operating models that enhance their ability to identify, monitor and manage third-party risks. Successful TPRM transformation demands strategies that overcome the roadblocks that have plagued systems

KPMG's framework for success in a new era

As we work with clients pursuing the development and implementation of TPRM programs for an unprecedented era of needs and challenges, we have developed a framework of key components for TPRM transformation that is built on four pillars: *Governance, Process, Infrastructure, Data*. Each has specific requirements, as illustrated below.

Governance

— 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

— 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

— 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 — and 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

— 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 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, 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.

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.

Our experience tells us that many FS companies still have a long way to go before they reach maturity, as illustrated by our survey findings. In our view, true transformation is driven by a *constant cycle* of program uplifts, process optimization and innovation. FS 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 determining where TPRM sits within the organization. This is ultimately decided by the nature and complexity of each business, though our research found that responsibility is most likely to fall under risk and compliance or finance, administration and operations. Within the latter group, organizations overall are increasingly identifying the procurement function to execute TPRM lifecycle activities. This can unlock significant operational efficiencies and an improved user experience for business relationship owners of third-party services. In doing so, however, a skillset uplift and cultural change may be required to prepare procurement to take on TPRM execution, as well as potential reporting line complications for third-party risk reporting to risk committees and Boards.

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.' Key to efficiency is a centralized and sustainable service-delivery model that facilitates risk assessment on behalf of, and with input from, the business. FS businesses may opt to use a distributed model, through which the business relationship manager coordinates inherent risk-assessment activities. There is, however, a higher cost to maintaining the distributed model amid the training and oversight required across vendor managers. Most often, we are seeing a trend toward a centralized model, where the centralized team executes risk assessment and provides outputs to the business-relationship managers, who finalize the decision to proceed with the third-party provider. Within the centralized model, FS businesses must also establish consistent oversight of fourth-parties, which is no small feat, given there is no direct contract between the organization and its fourth-parties.

Optimize the process: Ensure that third-parties failing to meet risk criteria and materiality thresholds are not put forward for assessment. Financial organizations can optimize the risk-stratification process in two ways: risk segmentation — establishing a disciplined risk-

scoring methodology across third-party services — and enhancement of the service-delivery model to reduce costs and increase accountability. These actions will help address the budget limitations flagged by survey respondents, as well as support TPRM teams in making smart, data-based decisions. Organizations should *segment* third-parties into three categories: Those presenting nominal risk to the organization and that do not need to be risk assessed; those that are appropriate for the standard TPRM process; and those that present a homogenous risk profile and are more efficiently managed centrally, via a specialty program. The aim here is to enable customization and tailoring for third parties that do not present the standard risk profile for risk-assessment requirements.

Evolve and innovate: FS TPRM programs typically revolve around the gathering and assessment of third-party data. The future will require financial organizations to rethink how data-driven, proactive risk monitoring via AI and machine learning will identify early-warning indicators for third-party resilience. We anticipate significant progress across two broad area: The sharing of due diligence responses across the industry, and the use of technology and scoring services to consistently assess third-party control environments. Most survey respondents told us they are leveraging or looking to leverage shared assessment information to reduce costs. With respect to TPRM technology innovation, our survey indicates that businesses overall are focusing their limited budgets on new tools. We see leading TPRM teams using automation, data analytics and natural language processing, as well as incorporating scoring services for affordable and scalable monitoring across select risk areas, performance management, and contract compliance. TPRM programs are exploring how they can use machine learning to evaluate internal data around risk events and identify risk events that may be caused by a third-party. They are automating the monitoring of third-party compliance with SLA terms, identifying opportunities to recoup fees for missed commitments, and taking a more-proactive approach to reputational risks.

In conclusion, our research confirms that FS organizations are rightfully viewing TPRM as a strategic priority. We see more businesses wisely taking a proactive approach to TPRM and exploring how they can refine and expand their existing processes through technology enablement and innovation. That said, our survey also makes clear that, for many organizations, TPRM remains a work in progress. Financial institutions have no time to lose in addressing the serious challenge of third-party risk and the pressing need for a more-consistent approach that ensures operational resilience. A risk-based approach is imperative — and businesses that delay the TPRM journey might do so at their own peril.

Contacts

Alexander Geschonneck
Partner
KPMG in Germany
T: +49 30 2068 1520
E: ageschonneck@kpmg.com

Sree Kunnath
Partner
KPMG in Canada
T: +1 416 791 2001
E: skunnath@kpmg.ca

Srinivas Potharaju
Partner
KPMG in India
T: +91 80 6833 5534
E: srinivasbp@kpmg.com

David Hicks
Partner
KPMG in the UK
T: +44 207 6942915
E: david.hicks@kpmg.co.uk

Greg Matthews
Partner
KPMG in the US
T: +1 201 621 1156
E: gmatthews1@kpmg.com

Gavin Rosettenstein
Director
KPMG Australia
T: +61 2 9335 8066
E: gavin1@kpmg.com.au

home.kpmg/socialmedia

Designed by Evalueserve.

Publication name: The TPRM journey continues for financial services businesses

Publication number: 137173-G

Publication date: November 2020