REPRINT

R&C risk & compliance

THIRD PARTY RISK MANAGEMENT: EVOLVING VENDOR, OPERATIONAL AND STRATEGIC RISKS

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2022 ISSUE

www.riskandcompliancemagazine.com

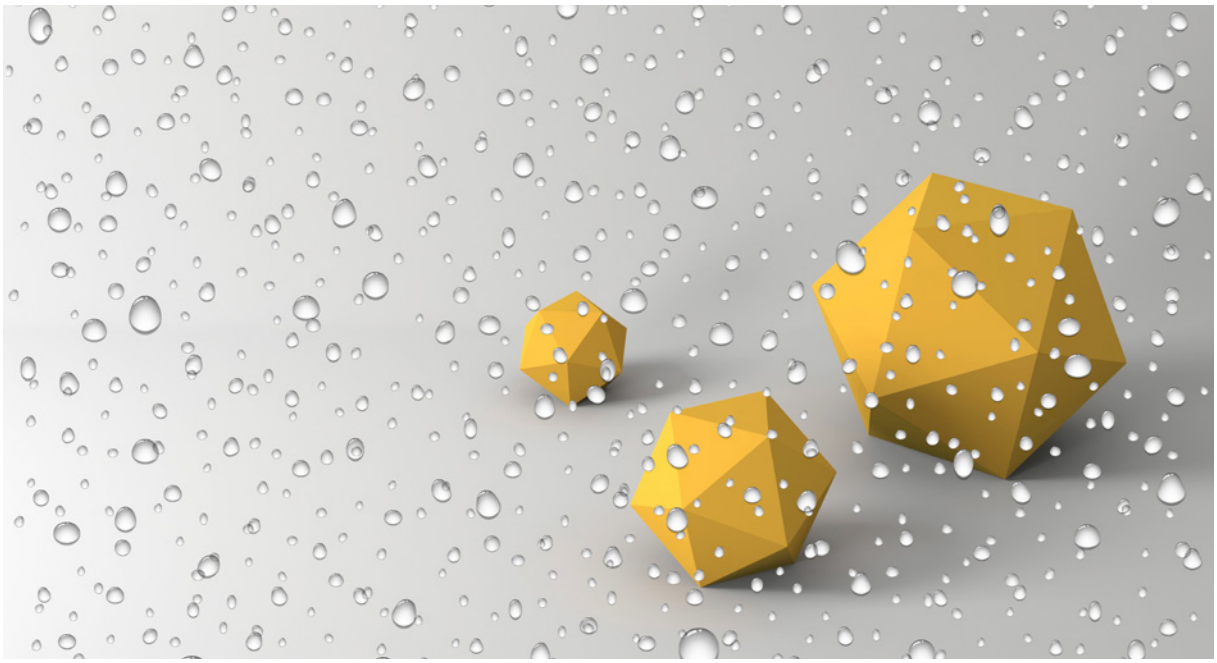
Visit the website to request
a free copy of the full e-magazine

KPMG

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

HOT TOPIC

THIRD PARTY RISK MANAGEMENT: EVOLVING VENDOR, OPERATIONAL AND STRATEGIC RISKS



PANEL EXPERTS

Greg Matthews
Partner, Regulatory and Compliance Risk
KPMG LLP
T: +1 (212) 954 7784
E: gmatthews1@kpmg.com

Greg Matthews is a partner with KPMG and has significant experience helping his clients transform their risk management operations based on regulatory and business drivers. He has worked with clients as they seek to manage disruption in their industry, meet regulatory expectations and use technology to drive both effective and efficient risk management practices. He brings his global experience to his clients to provide perspectives on how to implement changes in culture and balance risk and performance drivers. He leads third party risk management (TPRM) for KPMG.

Jon Dowie
Partner, Consulting
KPMG LLP
T: +44 (0)20 7311 5295
E: jon.dowie@kpmg.co.uk

Jon Dowie is a partner within the consulting practice at KPMG and leads its third party risk management (TPRM) practice in the UK. He has over 20 years of experience delivering and leading TPRM projects. His work often involves working with clients to help improve their maturity and comply with regulatory expectations and achieve TPRM transformation. He regularly works with the UK regulators, including the PRA and the FCA, on these topics, and is currently supporting a number of clients comply with PRA SS2/21.

Gavin Rosettenstein
Partner, Risk Strategy & Technology
KPMG
T: +61 2 9335 8066
E: gavin1@kpmg.com.au

Gavin Rosettenstein is a risk consulting partner and is KPMG Australia's National Leader for third party risk management (TPRM). He has over 17 years' experience in technology, governance and operational risk, TPRM, major risk and technology transformation, internal audit, strategic remediation and the setup and ongoing operations of risk functions.

R&C: Could you provide an overview of the kinds of vendor, operational and strategic risks associated with third-party relationships? How have these risks evolved in recent years?

Matthews: The risks associated with third-party relationships are extensions of any of the risks that a company experiences in its day-to-day operations, including financial, compliance, technology, information and cyber security. In addition, the use of a third party introduces the need for overseeing an external operation as if the third-party products and services were being done by internal operational units. The following scenarios exemplify how third-party risks are evolving. First, cyber security risk is top of mind across all industries, as firms seek to protect their information and services. In fact, the velocity of change is at an all high, with a number of high-profile ransomware attacks highlighting the reputational damage that can be done. Second, there is a general increased reliance on third parties as business operations evolve and digitalise. Ensuring that these increasingly complex services can be reliably delivered is driving the focus of management on operational resilience. A recent survey pointed out that three quarters of third party risk management (TPRM) executives identified their biggest reputational impacts come from a failure of third parties to deliver services in line with expectations. Third, there are increased regulatory requirements related to consumer protection, privacy, and environmental, social and governance (ESG) issues, which highlight the fact that companies can outsource anything but remain accountable for regulatory compliance. Another challenge comes from the increasing use of subcontractors or fourth parties and how to manage them indirectly, especially where the service involves other risk factors such as regulatory and compliance or cyber security risks.

> **"Technology selection and implementation should align with the complexity of the company's third-party risk profile, risk appetite and desired end-to-end process."**
>
> *John Dowie, KPMG LLP*

R&C: In your experience, do companies pay enough attention to due diligence when beginning new business relationships? Where does responsibility

for third-party risk management (TPRM) ultimately lie?

Dowie: Historically, companies generally carried out low levels of due diligence prior to contracting and instead relied on contractual terms as primary mitigating factors. As third-party risk awareness has increased, we have seen some companies and industries put more effort into this – however, this has led to an overly standard, 'one size fits all' approach. This has had a detrimental effect on costs and onboarding times. The bigger issue, though, is that this standardised approach does not allow for a proper assessment of the risks inherent in the service being purchased. This is resulting in companies not fully understanding the risks that they are going to be exposed to and not having an appropriate treatment strategy post contract in relation to the type and depth of ongoing activities based on the nature of the service or engagement. A TPRM function should be responsible for developing a TPRM programme that includes the definition of this risk-based approach. The function should be accountable for the facilitation of the TPRM lifecycle across many stakeholders, such as risk and control partners, procurement and business owners. Each of these stakeholders has certain responsibilities for parts of the TPRM programme as defined. We see that the TPRM programme generally sits either in the procurement team, which may sit under finance, or in the risk team, depending on the organisation.

R&C: In your experience, what types of third parties – be it suppliers, agents, intermediaries, advisers or consultants – typically pose the greatest risks to their business partners?

> **"The risk of a third party is determined less by spend or the type of service they provide, but more on how the service will be leveraged and relied upon by the organisation."**
>
> *Gavin Rosettenstein, KPMG*

Rosettenstein: The risk of a third party is determined less by spend or the type of service they provide, but more on how the service will be leveraged and relied upon by the organisation. Key risk factor considerations are often determined through the application of an inherent risk questionnaire (IRQ) to determine if specific risk factors exist within a proposed relationship. The IRQ

will determine the level of risk to the organisation, to which the appropriate safeguards need to be put in place to manage and mitigate those risks. Examples of IRQ questions include the following. First, if the third party becomes unavailable, will this impair the company's ability to meet stakeholder obligations and regulatory requirements? Second, what is the financial and operational impact on a company's reputation if a third party fails to perform over a given period of time? Third, how does a third party interact with customers or consumers on behalf of the company? Fourth, how does a third party access, process and store sensitive data, including personally identifiable information and a company's confidential, protected health information? Fifth, are services performed in certain jurisdictions considered a higher risk? Finally, what are the key risk issues associated with the use of subcontractors? The challenge for organisations in managing a broad array of third parties is often the volume and breadth of third-party inventory and the different types of risks that can be introduced based on those relationships. Organisations need to ensure the IRQ drives an effective and efficient way to identify and manage the risks that matter in a sustainable and measurable way.

R&C: How should companies go about creating a robust TPRM programme which effectively monitors and manages risk? What advice would you offer on assessing

risk levels, identifying red flags and monitoring a relationship over time?

Dowie: The TPRM team needs to establish a vision for the programme and define a target operating model for how the function will work. The foundation of an effective TPRM programme is a risk-based framework that defines roles and responsibilities for business users, risk groups, procurement and legal, among others. We would recommend a risk-based framework that uses an IRQ to identify and score materiality and risks, which then drives the breadth and depth of due diligence. Post-contract, due diligence results and inherent risk should drive the frequency and depth of ongoing monitoring activities. Without this sort of approach, you will not have a proportionate, risk-based framework, and you run the risk of not focusing on the things that matter most. Because TPRM programmes are complex, with multiple stakeholders engaged throughout the lifecycle, using technology to orchestrate the required activities can be the difference between success or failure. Technology selection and implementation should align with the complexity of the company's third-party risk profile, risk appetite and desired end-to-end process. Using technology to drive actions and workflow will also help track status and activities, as well as risks and issues, throughout the various phases of due diligence, contracting and ongoing monitoring. I would advise consideration of risk

intelligence sources to identify red flags, which can feed into the ongoing monitoring activities within the TPRM programme.

R&C: What specific challenges and risks do companies face when doing business with third parties in developing nations? To what extent is TPRM critical in this context?

Rosettenstein: When companies are looking to engage with or find they are conducting business with third parties that are domiciled or have operations within geographies of developing nations, key challenges that are faced include understanding risk factors that may be present, such as bribery or corruption impacting supply chain efficacy, the political or government climate that may impact data privacy, economic considerations such as fiscal and monetary policy and tariffs, as well as social considerations, including environmental impacts, immigration and labour policies, and ethnic or religious divisions. Any of these, among other geopolitical risk factors, could impair the successful and timely delivery of contractual obligations and meeting regulatory and legal requirements. These factors should be closely considered and managed when engaging third parties in different parts of the world.

R&C: If it becomes necessary, what steps should a company take to terminate a third-party relationship to avoid major disruption and reduce risk?

> **"Coordinating your oversight of a third party and driving a comprehensive view of the performance is important, and increased care should be placed on those relationships deemed critical."**
>
> *Greg Matthews, KPMG LLP*

Dowie: It is a mistake to think your relationship ends with the end of a contract. Returning data or having access to information in the event of an audit or regulatory inquiry can result in you having to continue working with your third party after the conclusion of the contract. Depending on whether you have a routine wind-up mechanism or an unplanned stressed termination can greatly impact the state of affairs. Either way, for higher-risk relationships, we encourage companies to start by planning for a termination during the onboarding process and require documentation of a more formal exit strategy. This is now becoming a regulatory

requirement in some jurisdictions. An exit strategy should include options, activities and relevant timelines that inform required activities in the event it is necessary to terminate or transition a third-party relationship. Options defined within an exit strategy often include the identification of back up providers of the products and services or what needs to be done to bring the service back in-house. The primary goals would be to make sure that services are not adversely impacted, and that data is secured and returned as appropriate.

R&C: As companies continue to seek business opportunities abroad, do you expect TPRM to become a core part of operational strategies? How is the process likely to evolve in the years ahead?

Matthews: For many organisations today, third parties are core to the delivery of their goods and services and as such the management of these relationships is core to the operational strategy. We read in the news of supply chain disruptions, and failures of third parties to deliver. Organisations are challenged to not manage third parties in silos, either via a business line or risk function. Coordinating your oversight of a third party and driving a comprehensive view of the performance is important, and increased care should be placed on those relationships deemed critical. Many organisations struggle with how to define the population to focus on and using their risk appetite is one way to understand where you should focus your efforts. So as TPRM integrates with other risk functions like enterprise risk management, compliance and cyber, clearly articulating how much risk you are willing to have a third party manage is key. Increasingly, we are seeing a focus on, inter and intra company transactions, many of which span global delivery and manufacturing hubs. Often this group of transactions represents the largest number of relationships that a particular legal entity may have. We expect to see an increased focused on aligning how you manage both external and internal relationships. R&C