KPMG

ForensicFocus

Managing third-party risk through effective due diligence

June 2018

Today's reality

Businesses across every industry are increasingly compelled to rely on a robust network of third parties, such as 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.

While third parties are imperative to operate globally, the risks associated with third parties cannot be outsourced. There are numerous cases where lack of proper oversight of third parties has resulted in serious consequences. Global companies have been exposed to significant risk, adversely affecting their performance and reputation.

Complying with regulators' demands

Regulators across the globe expect companies to have effective oversight of their third parties. Companies have had to prioritize and enhance their compliance efforts as a result of notable enforcement actions and fines due to instances of bribery and corruption, money laundering, and sanctions violations. In fact, a majority of reported Foreign Corrupt Practices Act (FCPA) cases have involved bribery through third-party intermediaries.

Various regulators focus on elements of the third-party life cycle (identification, risk assessment, due diligence, onboarding, and ongoing assessment) as they relate to the effectiveness of compliance programs. The U.S. Department of Justice (DOJ) and Securities and Exchange Commission (SEC) produced a joint guide[1] that stipulated how risk-based due diligence is particularly important with third parties and will be considered when assessing the effectiveness of a company's compliance program. In addition, the DOJ recently provided detailed guidance around the *Evaluation of Corporate Compliance Programs*[2].

The oversight and monitoring of the third-party life cycle has evolved from a reactionary approach to one of alignment to overall enterprise compliance programs. In order to achieve this congruence, ideal third-party risk management (TPRM) programs need to expand beyond the procurement function and encompass other stakeholders and departments across the enterprise. These programs will also gain maturity via automation—where the organization leverages data and an understanding of risk through technology to enhance management of third parties in a sustainable manner.

[1] https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf

[2] https://www.justice.gov/criminal-fraud/page/file/937501/download

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 786600

In a recent KPMG survey[3] of CCOs, a large number of respondents reported that they have not implemented leading practices to manage their third-party compliance risk.

Key challenges

There are a number of challenges faced by business leaders with respect to third-party risk management, such as:

- Difficulty in consistently identifying and managing third parties and associated risk assessments
- Time and expertise needed to implement robust, risk-based due diligence programs
- Lack of ability to demonstrate to regulators that appropriate oversight and controls are in place and work effectively
- Lack of visibility into third parties' business practices and risk/oversight functions
- Increased risk of data loss and customer privacy violations.

Regulators do not advocate a one-size-fits-all program. The approach and implementation of the TPRM program needs to align to a company's business needs, such as its size, complexities, and unique risk profile and appetite. At the same time, regulators want to see how a company's third-party management framework integrates a preventative and detective focus, while allowing for the three lines of defense[4] to operate holistically by adopting key governance elements across the TPRM life cycle.

The CCO perspective

In a recent initiative, KPMG spoke with chief compliance officers (CCOs) of FORTUNE 350 companies across all industries. Those CCOs discussed fundamental challenges, including understanding where and how data relating to third parties is best collected, how risk assessments should be conducted, and how information should be used across the enterprise—all while being able to manage the process in an effective, consistent, and efficient manner. As part of these discussions, specific business needs emerged:

- **Identification and management of third parties via a risk-based approach.** A key challenge to the third-party due diligence process is classifying the types of third parties and conducting a risk stratification exercise followed by regular monitoring and auditing of the relationships. The CCOs noted that conducting the same level of due diligence on all third parties would not be practical or cost effective. Therefore, by rating the third parties based upon defined criteria (i.e., the value of the relationship, the country risk, and the type of third party being sought), the company can identify a risk level that would further determine the level of due diligence required.
- **Integration of third-party processes between the business and compliance functions and clear definition of roles and responsibilities.** Some companies opted to have a decentralized model for onboarding and managing their third parties. However, this led to the development of many incongruous processes, straying from a consistent approach that a central compliance function would institute. The CCOs noted that the practical application of decision-making processes that involve business, compliance, legal, and ethics could be difficult. Therefore, a senior management committee should be put in place with the caveat that a compliance override could be implemented, if necessary.
- **Unified TPRM processes powered by strong technology solutions and automation.** Some CCOs expressed a challenge with manually intensive processes and a lack of automation. Older methods of assessing third parties, including third-party audit rights, are not economic or effective.

The due diligence pitfalls

Compliance and risk management functions can be overwhelmed with maintaining oversight within the organization itself and may not have the time, skills, or resources to maintain visibility over the company's third- or fourth-party network. As a result, inadequate levels of due diligence are conducted. Merely conducting sanctions and politically exposed persons (PEP) checks, or conducting basic Internet searches, typically do not return useful insights. In some cases, companies perform almost no checks other than obtaining self-reported information from third parties through onboarding questionnaires or credit reports, often to fulfill a "check the box" exercise with the hope of satisfying regulatory requirements.

[3] The three lines of defense are defined as 1st: the business, 2nd: compliance and risk management, 3rd: internal audit.

[4] https://advisory.kpmg.us/content/dam/kpmg-advisory/risk-consulting/pdfs/2017/03/compliance-journey-survey.pdf

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 786600

The World Economic Forum's Partnering Against Corruption Initiative (PACI)[5] divides the pre-onboarding process into three essential stages in its official guidelines for proper due diligence: (1) understanding the scope of the third-party universe, (2) performing risk assessment on individual entities to determine the amount of due diligence required, and (3) conducting said diligence. Additionally, the DOJ's and SEC's guide to the Foreign Corrupt Practices Act stipulates that companies must understand "the qualifications and associations of [their] third-party partners, including [their] business reputation."

Without ongoing, intelligent insight into a company's third-party network across the pre-onboarding, risk assessment, and post-performance phases, organizations leave themselves vulnerable to significant business, reputational, and compliance risks. It is paramount for companies to understand where the risks lie, how to identify the risks, and what measures they need to take to protect their brand and bottom line. These challenges bring to light new business challenges: the need to proactively assess, monitor, and manage the performance of third parties and implement robust processes to enforce this proactive behavior.

Leading due diligence trends

Better practices around TPRM advocate for a risk-based approach:

- **Establish scope.** Understand the universe of third-party relationships and performing risk analytics to determine those third parties that would be in scope for further review.
- **Build a risk assessment process.** Institute a risk assessment process that is differentiated by supplier tier and risk focus to determine appropriate levels of review on those third parties where further information is required.
- **Perform risk-based due diligence.** Based on the assessment, perform appropriate risk-based due diligence to obtain critical information to manage business risk.
- **Actively monitor and manage.** Continuously monitor and actively manage third parties, which will help answer key business questions: Should they do business with this third party? How is this third party performing? Should they continue to do business with this third party?

[5] http://www3.weforum.org/docs/WEF_PACI_ConductingThirdPartyDueDiligence_Guidelines_2013.pdf

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 786600

Integrating technology and data analytics

With the promulgation of more online data sources, the application of technology through machine learning techniques, and advanced analytics for research, initial risk assessments can be conducted on a higher volume of relationships in a smarter, faster, and cheaper way. Human analysis can be applied for due diligence on riskier third parties where initial results need interpretation, and further research can be expanded and analyzed as necessary. When automation and manual processes are integrated, companies have the ability to scale due diligence to a larger, if not an entire, network of third parties.

Such solutions could also be integrated with case management tools and other enterprise platforms, providing better insight into the universe of third parties and providing clarity of roles and responsibilities across lines of defense and risk oversight functions.

There are other transformative benefits involved as a result of implementing technology and data analysis:

- Alignment of TPRM policy and practices to procurement activities
- Development of a greater understanding of the organization's dependency on its third parties and their subcontractors
- Reduction in the redundancy of activities to assess third parties
- Development of a greater use of automation to manage third parties
- Implementation of consistent processes across the organization with regard to treatment of third parties
- Clarification of the cost-benefits analysis factoring in the true cost of oversight for services
- Improvement of board reporting with a comprehensive view of critical third parties, strategy, trends, and issues.

Moving forward

As long as companies continue to face complex risks in dynamic business environments and regulators continue to put pressure on companies to comply, it will remain critical for businesses to maintain a sustainable approach for any third-party risk management program to be successful.

Contact us

Amanda Rigby
Principal, U.S. Forensic Services Leader
T: 312-665-1953
E: amandarigby@kpmg.com

Authors
Jilane Khakhar and Zehra Venugopal

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

kpmg.com/socialmedia

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.

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 786600