KPMG

Managing third party risks

You are only as strong as your weakest link...

#RiskMatters

With increasing business complexity, associating with third parties is only logical considering benefits such as lower costs, better operational efficiency, special expertise, newer and robust technology implementation, economies of scale etc. But are you sure that in a bid to get these benefits, your business is not opening doors to someone who can do more harm than good to your business?

As per a recent study conducted by one of the world's leading research organisation in 2020, over 80 per cent of legal and compliance leaders believe that third-party risks were recognized after initial onboarding and due diligence. This implies that conventional due diligence methods in risk management policy are unable to capture new and emerging risks.

The ever-increasing business relationships with third parties are no longer restricted to outsourcing but have transformed into an extended arm of the organisation itself, in turn exposing them to a greater risk universe.

- **A recent cyber-attack on an airline data service provider resulted in data leakage of personal data of 4.5 million passengers worldwide. The data set was not only limited to name, contact information but also passport details, ticket information, and credit card details**
- **Earlier in January 2020, a private airline suffered a data breach that led to the compromise of 1.2 million passenger records.**

Questions to consider

01 Do we have the right governance model to continuously monitor third-party risks?

Including but not limited to:

- A clear definition of third parties and visibility of the associated risk exposure?
- Do we have the mechanism to mitigate and respond to third-party risk crisis?
- What coverage do we have to address four-party subcontractor risks?
- What is our plan to recover from a potential third-party risk crisis?
- Do we have clear roles and responsibilities for third-party risk management?
- Do we have a codified process to identify, assess, manage, monitor and terminate third parties?
- A defined outsourcing and third-party strategy along with risk appetite?
- Does Third Party Risk Management program promote ESG agenda for a responsible supply chain?

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

02 Do we have the right process framework to manage and mitigate third party risks?

Including but not limited to:

- Is there consistency in execution of TPRM program across the organisation?
- An assessment team with right skillsets, expertise, and bandwidth?
- Process to undertake risk assessment before contract execution and decision making?
- Adequate focus on continued risk analysis and mitigation rather than data collation and survey – response gathering?
- Tracking the contract validity on continuous basis? Do you have templates that drive consistency across the organisation?

03 Do we have the right data to make informed third party-related decisions?

Including but not limited to:

- A wide-ranging data model for collation of third-party information?
- Internal and external data feeds to monitor and capture adverse information relating to specific events and incidents attributable to third parties?
- Do we have system of real time tracking of performance against defined SLAs?
- Are you making informed decisions based on advanced data analytics?

04 Do we have the right infrastructure to ensure a stable and smooth running TPRM program?

Including but not limited to:

- Is the TPRM program driven by ERM?
- Does TPRM program adequately safeguard all stakeholder interests and is it aligned with regulatory requirements?
- Are you leveraging multiple automation options including process automation, analytics and contract intelligence as part of TPRM program?
- Do we have an audit trail that is documented and well understood?
- Is the service delivery model well aligned with organisation's operating style?

Third party risk universe

Compliance risk
Non-compliance with statutory and regulatory framework

Concentration risk
Supplier concentration across critical services & skills

Contractual risk
Unfavorable clauses, insufficient coverage of all clauses in third party contracts

Cyber risk
Data leakage and security breach from third parties' database

Environmental, social & governance (ESG) risk
Higher scrutiny from regulators amid increased awareness towards climate sustainability

Financial risk
Inability to fulfill contractual obligations putting the third parties' going concern status under a cloud

Fourth-party risk
Insufficiencies with vendors transacting with third parties

Fraud, bribery & corruption risk
Frauds and misconduct by third parties

Geopolitical risk
Unsuitable geographical and political business environment

Operational/supply chain risk
Inadequate services leading to supply chain disruptions which can further lead to threats to business continuity

Reputational risk
Industrial espionage due to third parties' misfunction

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Where do we start?

Underlying technology layer

01

On-boarding

Approvals from business, Information security, procurement, and compliance teams. Have an on-boarding checklist and the same should be followed.

02

Conduct due diligence

Determine control effectiveness by doing third party due diligence with an in-depth understanding of areas like IT security, financial stability, corruption, bribery etc.

03

Third party identification and risk assessment

Understand why third-party services are required along with extent of reliance on them. Create a central database to identify, assess and profile risks

04

Classification and service risk profiling

Classify the third parties into service categories and determine the risk of these service categories for service risk profiling

05

Risk acceptance

Prepare a mitigation plan that keeps residual risk within the organisation's overall risk appetite

06

Contract management

Based on the risks identified, develop a third-party contract management system which targets continuous monitoring of key contractual clauses

Ongoing third-party portfolio viability

Periodic reviews and updating of centralised third-party data pool for better risk profiling and mitigation

07

Ongoing performance evaluation

Develop performance scorecards with defined KPIs

08

Risk evaluation and mitigation

Review the risk evaluation and mitigation plan to ensure residual risk is within risk tolerance limit

09

Off-boarding

Conduct review at the end of contract to assess compliance with requirements

10

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

How to optimise your existing TPRM program?

The TPRM program is an ongoing and continuous process. It is driven by constant program uplifts, process optimisations and innovations:

Developing vision

- Budgetary allocation of funds to evolve and strengthen the TPRM program
- Designating ownership and identifying where TPRM program fits within the organisation
- Determining aspirants for automation.

Build the model

- Deciding the involvement of stakeholders throughout the TPRM lifecycle
- Determining whether a centralised or decentralised model should be used for performing risk assessment activities.

Process optimization

- To optimize TPRM program, third parties that fail to meet predetermined risk criteria and materiality thresholds shouldn't be considered for risk assessment. Risk stratification process can be optimized in the following ways:
  - Risk segmentation: Creating a strict risk scoring methodology across third party services
  - Improving the service delivery model to minimise costs and maximise accountability
- Continuous training and skill development for the TPRM program is of utmost importance to combat the talent challenges faced in risk segmentation process.

Evolve and innovate:

- Information sharing of one-time third-party risk assessment through a centralized aggregator might result in free flow of information across the organisation and will avoid confusion
- Viability of leveraging new technology should be investigated for enhancement of TPRM program
- Look at automation of manual processes to manage the TPRM function in efficient manner.

In summary, there is a critical need to carefully screen and assess the components listed above to manage the evolving risks being posed by third parties. Companies need to look for an automated third-party risk management solution and embed a comprehensive framework which addresses these key tenets of an effective third-party risk management and provides adequate visibility and transparency to senior management, auditors, and regulators.

KPMG in India contacts:

Vijay Chawla
Partner and Head
Risk Advisory
T: +91 80683 35509
E: vschawla@kpmg.com

Ritesh Tiwari
Partner
Risk Advisory,
Leader – Board Leadership Center
T: +91 124 336 9473
E: riteshtiwari@kpmg.com

Shivani Sanwal
Director
Governance, Risk and Compliance Services
T: +91 98199 54752
E: shivanisanwal@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/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 on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG (Registered) (a partnership firm with Registration No. BA-62445) converted into KPMG Assurance and Consulting Services LLP (a Limited Liability partnership firm) with LLP Registration No. AAT-0367 with effect from July 23, 2020.

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

This document is for e-communication only. (015_FLY0721_SP)