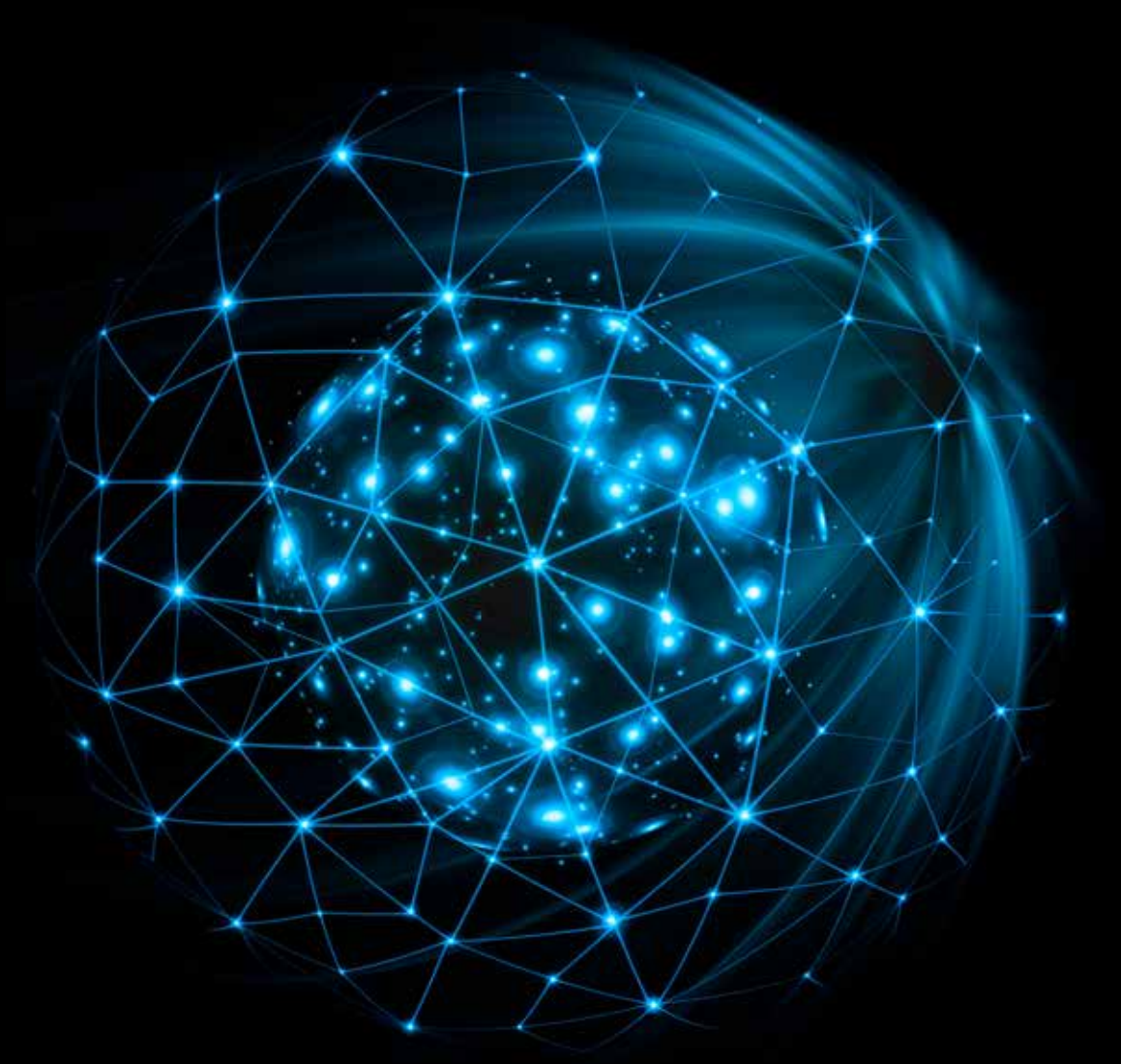
Deloitte.



Third-party risk management

September 2023

Introduction

In today's interconnected and globalised business landscape, most organisations rely on third-parties to achieve operational efficiency and competitiveness. However, the increased reliance can expose organisations to several risks with severe consequences.

Third-party vendors (individuals/entities) that interact with government authorities/officials for/on behalf of an organisation are also known as “Third-Party Intermediaries” (TPI).

Regulators across the world understand the bribery and corruption risks posed by TPIs. About 90 percent of the enforcement actions taken under the Foreign Corrupt Practices Act (FCPA) involve using a TPI,[1] such as agents, consultants, and distributors, to conceal bribe payments made to government officials.

Anti-corruption legislation of various jurisdictions prohibits not only direct corrupt payments to a foreign official/ government official to obtain or retain a business but also any form of indirect corrupt payments made through such TPIs.

The US Department of Justice (DOJ) and the Securities and Exchange Commission’s (SEC) resource guide to the US FCPA (Guide) suggests that a US organisation conducting business through TPIs should perform a risk-based evaluation of these intermediaries based on the nature of the business relationship.[2]

Third-party due diligence can help ensure anti-corruption compliance and safeguard an organisation's reputation and financial well-being. Most organisations and compliance professionals understand the need to comply with the requirements of conducting due diligence on TPIs. However, one common challenge that compliance professionals face is creating a robust third-party risk management framework and maintaining a repository of risks from such TPIs.

Hence, it is important not just to identify the risks associated with TPIs prior to onboarding but also through the entire lifespan of the TPI’s relationship with the organisation. The degree of risk management may vary based on industry, country, size, and nature of the organisation, TPI, and the transaction itself.

Today, regulatory bodies expect organisations to undergo these basic diligence checks, along with having a robust compliance framework. These steps will help them mitigate bribery and corruption risks that may arise while engaging with TPIs.

[1] https://fcpa.stanford.edu/statistics-analytics.html?tab=4
[2] https://www.justice.gov/criminal-fraud/fcpa-resource-guide

Key guiding principles

An effective third-party risk management framework may include some of the practices mentioned below:

Identification and risk classification

Organisations need to identify the business rationale for third-party relationships and assign a risk category on the basis of the potential bribery and corruption risk they could pose. This should also be mapped to the criticality to the business. Potential bribery and corruption risks may depend on various factors, such as jurisdiction, nature of operation, value, and interaction with government departments/officials. For example, getting a change of land use certificate from district authorities could be a high-risk activity compared with applying for a licence through an online portal. Such a risk categorisation (high, medium, low) helps prioritise organisational resources and efforts towards more effective risk management. Organisations should also check if the TPI will use a sub-contractor to perform any service.

Due diligence (DD)

Depending on the risk categorisation of the TPI or sub-contractor, the appropriate level of DD (basic, intermediate, or advanced) must be conducted on TPIs. DD questionnaires are usually designed to obtain information, such as shareholders, directors, related companies, relationships with government officials, current or previous employment with government authorities, and use of subcontractors.

A DD exercise focuses on identifying and responding to some key aspects of TPIs. Some of these are mentioned below.

- Substantiating the legitimacy and reputation of the TPI, its directors, and key shareholders
- Gathering information on ongoing litigation matters (civil/criminal) against the TPI and/or subcontractor
- Understanding if there are any adverse issues, such as disqualifications, defaults, disputes, and public grievances
- Uncovering if the TPI has a history of engaging in fraudulent or unethical/illegal practices
- Gathering information on any concerns related to:
  - financial health, loan repayment defaults, money laundering, siphoning of funds, and other financial crimes;
  - whether the TPI is owned (including the ultimate beneficial owner) by Politically Exposed Persons (PEP) or connected directly or indirectly with a PEP;
  - regulatory defaults; and
  - presence on sanctions/watch lists.

Compliance officers or organisations may have to modify risk categorisation on the basis of the results of the DD. Any observations/issues identified during the DD are either resolved or an appropriate remediation plan is prepared and implemented. Further, organisations should have a framework in place to refresh the TPI DD regularly depending on the risk ranking, observations noted during the DD, the quantum of transactions, and/or other external factors leading to a change in TPI management.

Contractual safeguards

Written contracts with TPIs are a critical anti-corruption mitigation strategy that documents the scope of work, expectations, and obligations of TPI, along with defining an organisation's rights with respect to business relationships.

Contractual provisions assist organisations in preventing and detecting bribery and corruption. In case of an incident, these provisions act as a tool for consequence management.

- **Preventing bribery and corruption:** Contractual provisions prohibit bribery and corruption by enforcing anti-corruption laws (Prevention of Corruption Act, FCPA, UKBA, etc.) and the organisation's code of conduct on TPIs. In addition, it demonstrates the organisation's commitment towards compliance.
- **Detecting instances of bribery and corruption:** Contractual provisions, such as "Right to Audit" help organisations conduct audit reviews of TPIs' books of accounts to detect any potential irregularities.
- **Consequence management:** This safeguards the organisation's interest using provisions such as the "Right to Terminate" in case any misconduct is identified, and certifications from TPIs that they have acted in compliance with anti-corruption laws (thereby protecting the interest and reputation of businesses.

Training of TPIs

After finalising the contract and before taking any services from TPI, organisations should ensure that the TPI is trained on their anti-corruption policies, applicable laws, and regulations. Training helps clarify specific procedural requirements that the TPI needs to comply with during its association with the organisation.

Review of invoices and processing payments to TPIs

Once services are provided and the invoice is received from the TPI, organisations should ensure that the invoice, along with supporting documents, is reviewed for any red flags. Organisations should also ensure that payments to the TPI are processed through official banking channels to the intermediary's authorised bank accounts.

Some common red flags that could be identified while reviewing invoices and processing payments are mentioned below:

- Requests for reimbursement of fees and/ or expenses with limited documentation or evidence of services performed
- Vendor payments inconsistent with contract terms
- Upfront payments and deposits requested by the vendor to secure business
- Unusually high commissions, large credit lines, free products/services, and discounts granted to distributors
- TPIs that are incorporated or established in an offshore jurisdiction
- TPI to request payments through an offshore/ bank account of someone else
- Unreasonable discounts to third-party distributors
- TPI provides services that are in deviation to the services described in the contract

TPI audits

Monitoring TPI transactions and activities ensures that the intermediary complies with the requisite anti-corruption laws and policies, and organismal procedures. TPI audits provide an opportunity to stress test that the TPI is performing activities in compliance with the contract and relevant laws, and within the boundaries set by the organisation. Such audits also help demonstrate an organisation's commitment towards compliance and help identify improvement opportunities for the TPI.

TPI database management

No TPI risk management framework would be complete without a comprehensive database. The database has relevant details, such as TPI's name, key management, nature of services performed, risk category, date of appointment, DD status, date of latest DD, date when the contract was executed/ revised, the department availing services, and TPI SPOC. It also has other details related to the TPI's engagement with the organisation. Such a database will help the organisation perform the above-mentioned aspects, such as TPI audit, risk categorisation, refreshing the DD, and training. The database will also assist in off-boarding/ rejecting TPIs, should a situation arise.

Conclusion

Creating a third-party risk management framework could be a complex exercise – one that is no longer optional but a fundamental necessity for businesses operating in a heavily regulated and interconnected world. Identifying the degree of required risk management (based on industry, geography, size, and nature of the transaction) is difficult as businesses continue to scale and collaborate with third parties. This makes third-party risk management critical.

By proactively identifying and addressing risks associated with third-party relationships, organisations can not only adhere to the laws but also safeguard their reputation, financial stability, and long-term success in a competitive marketplace.

Connect with us

Nikhil Bedi
Partner and Leader - Forensic
Financial Advisory
Deloitte India
nikhilbedi@deloitte.com

Aakash Sharma
Partner - Forensic
Financial Advisory
Deloitte India
aakashsharma@deloitte.com

Saurabh Khosla
Partner - Forensic
Financial Advisory
Deloitte India
khoslas@deloitte.com

Contributors

Lokesh Chopra
Shobhit Jain

Deloitte.