Diligent

Five Steps to Implementing a Risk-Based Due Diligence Program

Introduction

Greater enforcement of Anti-Bribery and Anti-Corruption (ABAC) laws around the world have increased the scope of corporate compliance department responsibilities. A major element of any corporate ABAC program involves the performance of due diligence on third-party intermediaries. And for good reason, regulators routinely uncover evidence that a corrupt act was committed by an intermediary acting on the company's behalf, both with and without the company's knowledge. According to an analysis conducted by Foreign Corrupt Practices Clearing House, more than 90% of investiga-tions and enforcement activity related to FCPA bribery cases over the past ten years involved a third-party.[1]

Performing risk-based due diligence on intermediaries has become a critical practice for companies to confidently mitigate third-party risks. While all misconduct cannot be eliminated through a compliance program, ABAC enforcement entities consistently emphasize that due diligence is key to a well-designed and effective compliance program.

Assigning the appropriate level of due diligence for the company's third parties requires assessing risks objectively and systematically. In order to build a credible and practical risk model, company executives must understand concretely how the company operates across its business units, regions, and subsidiaries.

While debate remains around how much due diligence to conduct and how often, there is no debate as to the necessity of a risk-based approach to diligence. A company board, officers, and employees cannot choose to abstain from performing third-party diligence, either. The era of turning a blind eye is behind us. In fact, there have been several instances in which individuals and companies have been prosecuted and convicted where actual knowledge of payments was not present. Building a credible ABAC program is paramount in protecting corporate reputation, shielding executives and management from personal and professional liability.

Growing evidence suggests companies with a reputation for having a good ABAC program benefit from being able to attract investors and customers because they are seen as more transparent and ethically-oriented.[2]

> "Possessing a robust compliance program can protect corporate reputation, shield executives, board members, and other management from personal and professional liability and provide significant competitive advantage in a challenging global business environment."

Diligent

Risk-Based Due Diligence: The Challenge

Despite recognizing the significant risks posed to companies by intermediary relationships, and the need for riskbased due diligence, it is a struggle for businesses and their compliance teams to effectively onboard third parties and manage and monitor risk on an on-going basis.

This is overwhelmingly due to two main reasons:

1. The sheer volume of third parties that most large companies engage
2. The complexity of identifying and collecting information across business units and regions with different cultures, political climates and norms

The complexity and volume make risk identification and mitigation in relation to business partners and intermediaries—the cornerstones of a risk-based ABAC approach—a constant challenge. As a consequence, the value and purpose of a risk-based approach is an important step in building credibility in the compliance program.

Lay a Strong Foundation Through Stake-holder Alignment

The process of creating a sustainable risk-based ABAC program involves several steps. Key components for a risk-based ABAC program are outlined in the DOJ and SEC's Resource Guide on FCPA (recently revised in July 2020; "the 2020 FCPA Resource Guide") and the DOJ's June 2020 guidance for prosecutors on Evaluation of Corporate Compliance Programs ("DOJ's June 2020 Guidance"). The first step is identifying the stakeholders to participate in the development, roll out, and ongoing monitoring of the program. This must include key business leaders, general counsel, the compliance officer and compliance staff, and likely member(s) of internal audit, procurement and IT.

Engaging stakeholders from the outset and on a consistent basis is key to creating the culture of compliance and ensuring that it is well resourced. It is clear from the DOJ's June 2020 Guidance that regulators will look to the good faith and earnest efforts made within a company to design and implement an ABAC program. Good faith effort is considered in light of how well the program is resourced by the company so it can be effective. This includes the tone set by senior management and mid-level management in informing employees in practical terms how to comply and ensuring that inappropriate activity is properly reported and addressed. In furtherance of this, the 2020 FCPA Resource Guide identifies that the truest measure of effectiveness of a company's compliance program is how it responds to misconduct - there should be a well-functioning and adequately funded mechanism for investigations of allegations of misconduct by the company, its employees, or agents.

Importantly, without involvement from the sales and business development teams, the process will be challenged from the start. After all, the business development team knows the business process with which the compliance process will need to integrate.

> "Recognizing and being able to articulate the value and purpose of a risk-based approach is an important step in building credibility in the compliance program."

Diligent

A Step-by-Step Approach to Implementing a Risk-Based Program

From our experience, implementing a risk-based approach to third-party management generally involves the following steps:

Step One: Develop a Risk Inventory

Aggregate third-party data across all IT systems. Normalize the data and cleanse it for duplicates and errors, then determine the type and purpose of the relationship. There will likely be many more third parties than originally estimated. This may be particularly difficult for larger multinational corporations which grow through acquisitions. In most instances subsidiaries will have different data sources and systems which need to be aggregated and normalized for use in an enterprise wide compliance program.

Examine ERP and CRM systems, accounts payable records, point-of-sale data, business reviews, interviews and any other source that may reveal use of an intermediary. Often a company is not aware of the relationships that a third party may have or the intermediaries that the third-party uses for business processes. It is beneficial to consider an expansive definition of third party for purposes of developing the risk inventory. The process must be as robust as possible, automated, and run continuously to capture and include newly added third-party relationships.

Step Two: Perform an Initial Risk Assessment and Create Third-Party Risk Profiles

Determine the general risks that may be posed by the intermediary. Is it in a country known to be a high risk for corruption? How much business does it do with the company? Is it performing services in a type of industry known to be high-risk for corruption? What percentage of the intermediary's business depends on your business? What is the compensation structure? Does it interact with government officials? Is the company state-owned or do its senior managers have close ties to government officials? What is the reputation of the entity in-country? Did they follow selection process? There are approximately two dozen common risk factors that most companies will consider for inclusion in their risk calculation, but the key is to select only those risk factors that are consistently captured or carried out in the company's business process, since including a risk factor that is only relevant some of the time can skew the risk score calculation. Based on the risk calculation, third parties should be associated with a risk profile and tier that has a prescribed scope of due diligence.

Diligent

Step Three: Conduct Investigative Due Diligence

Address those third parties identified through the risk assessment as the high-risk category first. This is where most resources should be spent. Those in the low-risk category can be assessed later in the process. Allocating resources in this manner will ensure the most efficient use of time and money and, based on our knowledge and experience, will be viewed favorably by the DOJ and SEC. When conducting due diligence on a third-party intermediary, there are several considerations that should be addressed: nature of the services being delivered and clear rationale for the third-party, shareholder and management identification, relationships with government officials, the intermediary's use of third parties, historical compliance issues, conflicts of interest, and the third-party's internal control structures. These considerations provide a good foundation for diligence efforts regardless of the size or nature of business of the company. Per the 2020 FCPA Resource Guide, the FCPA expressly prohibits corrupt payments made through third parties or intermediaries, whether there is, or should have been, actual knowledge on the part of the corporate entity. Information gathering is key to an effective, risk-based compliance program.

Step Four: Resolve Red Flags

Address red flags or deficiencies identified during the due diligence phase. In some extreme cases, it will be more efficient to sever ties and walk away, but often it is possible to remedy issues with the third-party by providing training, contract revisions and other steps. A robust and auditable investigation conducted in line with the company's anti-corruption policy is required to ensure a credible and defensible program.

Resolving red flags has to be consistent with the overarching concept of deterrence and providing concrete incentives for compliance. When engaging new third-par-ties, particularly those for whom a thorough investigative process is not possible, consider including contract terms that clearly allow for ABAC specific audits, certification requirements, and contract termination provisions for misconduct.

Additionally, ensure that your compliance program incorporates mechanisms that allow for tracking of red flags over time, so that the third-party is not hired or re-hired at a future date.

Step Five: Commit to Ongoing Monitoring

Depending on the nature of the relationship and the level of risk, it will be necessary to monitor and reevaluate existing third parties on a regular basis. Regulators have indicated clearly that they will take into consideration how well a company's compliance program monitors third-par-ties beyond the initial onboarding process.

Expect that risk profiles will change as some lowerrisk vendors may become higher risk in the future while highrisk intermediaries must be reviewed frequently to ensure compliance with established terms and conditions.

Periodically test your program to determine if it continues to expose areas of risk and provide possibilities for mitigation. In testing the program to ensure that compliance efforts are commensurate with the risks it is important for the compliance team to have continuous access to operational data and that policies and procedures reflect ongoing changes.

In addition, ongoing review and monitoring should take into consideration lessons learned within the company and the industry and how access to changes in policy or procedures are disseminated and implemented within the company.

Diligent

Risk-Based Due Diligence Is Essential

Corporations that implement effective risk-based third-party due diligence programs are demonstrating to regulators that they are serious about tackling corruption. With energetic enforcement by regulatory agencies around the globe expected to continue to increase, the risk to companies, executives, and boards of directors continues to rise. Possessing a robust compliance program can protect corporate reputation, shield executives, board members, and other management from personal and professional liability and provide significant competitive advantage in a challenging global business environment. Both the DOJ's June 2020 Guide and 2020 FCPA Resource Guide incentivize organizations to have robust, well-struc-tured, and evolving compliance programs in place before an occurrence or violation.

While it is important to follow the structure of a program as outlined here, each company has a different appetite for risk based on its industry, size, and the countries in which it operates. Therefore, no two compliance and risk models will be identical. There must be a degree of customization and flexibility to ensure that a riskbased compliance program fits a company's culture, risk appetite, and budget.

Resources:

[1] Third-party intermediaries, Foreign Corrupt Practice Clearing House Act, available at: **http://fcpa.stanford.edu/ chart-intermediary.html**.

[2] Ravi Venkatesan and Leslie Benton, How Companies Can Take a Stand Against Bribery, Harvard Business Reviews, available at: **https://hbr.org/2018/09/how-companies-can-takea-stand-against-bribery**.