Diligent

Third-Party Due Diligence: Creating a Credible & Defensible Program

Introduction

Ensuring compliance with anti-corruption statutes such as the U.S. Foreign Corrupt Practices Act ("FCPA") or the U.K. Bribery Act is a complex task. That is all the more true particularly for how organizations oversee the third parties acting on their behalf.

The cornerstones for third-party oversight are due diligence and monitoring—but building those concepts into a credible compliance program requires a multi-pronged effort; one that aligns an organization's people, processes, and technology to prevent and detect violations.

What's more, achieving that credible third-party program remains an urgent compliance priority, as is spelled out in multiple guidance documents from the US Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC"). The DOJ and SEC's Guide to the U.S. Foreign Corrupt Practices Act, Second Edition ("The FCPA Resource Guide," last revised July 2020) continues to be a blueprint for effective compliance programs today. One section contained this passage about third-party due diligence:

DOJ's and SEC's FCPA enforcement actions demonstrate that third parties, including agents, consultants, and distributors, are commonly used to conceal the payment of bribes to foreign officials in international business transactions. Risk-based due diligence is particularly important with third parties and will also be considered by DOJ and SEC in assessing the effectiveness of a company's compliance program.[1]

In other words, if a third party violates the law on your behalf, the absence of authorization from your company, combined with a credible and defensible compliance program, will send a strong message to regulators about your company's commitment to compliance. Those elements cannot guarantee the avoidance of criminal prosecution, but they do firmly tilt the company toward that outcome.

As stated in the DOJ's June 2020 updated guidance to prosecutors on Evaluation of Corporate Compliance programs ("DOJ's 2020 Guidance,") regulators will look to see if the compliance program is risk-based, proportionality resourced, data-driven, and regularly reviewed. Both the DOJ's June 2020 Guide and 2020 FCPA Resource Guide incentivize organizations to have robust, well-structured, and evolving compliance programs in place before an occurrence or violation.

Diligent

Specifically, in relation to third-party compliance, regulators will evaluate the program based on whether it is risk-based, whether the risk-based analysis is integrated into business processes, that there are appropriate controls which are periodically evaluated to adapt to lessons learned, and that the incentive structures and relationships related to the third party are evaluated and regularly re-evaluated, with concrete action taken to address revealed misconduct.

This paper provides an overview of the standards and principles related to the systematic vetting of third parties such as resellers, agents, distributors, sales and marketing representatives, and joint venture partners.

Third-Party Due Diligence and Management Defined

Anti-bribery and anti-corruption compliance programs vary from company to company, region to region, and industry to industry. Developing the right compliance program for your own business can hinge on numerous factors, including internal culture, market imperatives, and executive leadership. What works well for one company may not work for another, even if they are in the same industry or of similar size.

The FCPA Resource Guide even acknowledges this:

Individual companies may have different compliance needs depending on their size and the particular risks associated with their businesses, among other factors. When it comes to compliance, there is no one-size-fits-all program.[2]

This is re-iterated in the DOJ's 2020 Guidance to prosecutors where it states that the need for and depth of due diligence efforts conducted by the company depends on the size and nature of the company, the type of transaction, and the third-party.

That said, the fundamental goal of any compliance program is universal: to prevent and detect corruption, without creating unnecessary administrative and budgetary burdens. Drill deeper into that idea, and three more specific goals emerge for third-party management:

- Understand the qualifications and associations of third-party partners, including a party's business reputation and its relationship (if any) with foreign governments or officials. The degree of scrutiny a company applies should increase as more red flags surface.
- Understand the business rationale for working with the third party and the incentive structures. Among other things, the company should understand why the third party is necessary at all and what service the party performs; and ensure that contract terms specifically describe those services rendered.
- Undertake ongoing monitoring of third-party relationships. Incorporating mechanisms to monitor the continued rationale for the relationship, incentive structure, and associations of the third-party for the lifespan of the relationship. This may include periodically renewing due diligence, evaluating the risks associated with a participation compensation and incentive structure, exercising audit rights, providing periodic training, and requesting annual compliance certifications by the third party.

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. This means that due diligence and management of third-party relationships is not just about knowing your company's business partners; it's about knowing who in your own company is responsible for the relationship and how they monitor the relationship on an ongoing basis. To conduct effective third-party due diligence and management, companies must answer the following questions:

- Will the company itself perform third-party due diligence, or will it engage a suitably qualified advisory firm?
- Which department within the company will manage or oversee the third-party due diligence effort?
- Is the department responsible for oversight of third-party due diligence well-resourced and given sufficient power to make consistent decisions regarding third-party compliance?
- How will the company communicate its commitment to anti-corruption laws to its employees, stakeholders, and third parties?
- How will the company measure the effectiveness of its compliance efforts?
- Will the company apply a uniform approach to third-party due diligence in all of its markets, or apply a risk-based approach that assesses the inherent risk in each market and the exposure to each third party?
- Are software and data-driven solutions available to help manage the third-party due diligence effort?
- How will the company track red flags and ensure that the parties it screens out or terminates a relationship with are not hired or re-hired?

Where and When to Begin

Prior to signing an agreement with a third party, your compliance team (or suitably qualified risk advisory firm) must complete the appropriate level of due diligence. That includes a review of relevant business records to ensure that the third party's activities to date reflect your organization's commitment to anti-bribery laws. When your company enters into a business relationship with an agent, distributor, joint venture partner, or any third-party intermediary, compliance managers should ensure that those counterparties, as well as the attorney representing your interests in the negotiation, clearly understand applicable anti-bribery law.

That review must be thoughtful and competent. A third- party due diligence program will likely not meet regulators' expectations if it only includes a review of sanction and embargo databases plus basic internet searches. As we said earlier, federal enforcement authorities expect companies to develop, monitor, and evolve a third-party due diligence and management program customized to reflect the organization's unique risks and operating environment.

As a practical matter, however, a third-party management program can easily become cost-prohibitive and present a significant administrative burden if companies charge forward with manual processes; there is simply too much information to find, digest, and track. A well designed and executed compliance program, on the other hand, can satisfy regulatory demands in a much more cost-effective way.

Due diligence programs also become more cost-effective when the company embraces a risk-based approach: focusing more of its resources on those parties, markets, and transactions that pose more risk. The FCPA Resource Guide assures companies that they won't be faulted for taking a risk-based approach to either third parties specifically or compliance in general.

DOJ and SEC will give meaningful credit to a company that implements in good faith a comprehensive, risk-based compliance program, even if that program does not prevent an infraction in a low-risk area because greater attention and resources had been devoted to a higher risk area.

In addition, the DOJ and SEC will assess whether a company has informed third parties of its compliance program and commitment to ethical and lawful business practices and, where appropriate, whether it has provided training and sought assurances from third parties, through certifications and otherwise, of reciprocal commitments.

Diligent

Consistent with the DOJ/SEC's guidance, Diligent's experience with over 200 multinational companies indicates that the majority employ a risk-based approach. Based on the DOJ/SEC Guidance noted above, as well as our experiences with clients around the globe, we view risk-based third-party due diligence as critical to ensuring regulatory compliance.

Levels of Due Diligence

An effective due diligence program takes steps to understand the extent of business relationships within the company's markets, as well as an assessment of all business transactions (both domestically and overseas) and the individuals involved.

The initial assessment seeks to achieve two things.

First, identify all foreign third parties, which can include resellers, lobbyists, customs liaisons, distributors, supply chain representatives, joint venture partners, consultants, and targets of acquisition. Next, assess the level of FCPA or anti-bribery and anti-corruption law training and awareness among third parties, especially for overseas third parties that may not have been required to comply with the law in the past.

Once the company has that inventory of third parties and the FCPA awareness they do or don't have, it can proceed to a more detailed assessment of each third party. That detailed assessment will ask questions such as:

- What is each third party's legal name, address, and ownership structure?
- Who are the principals? What information is shown on the organization's website? What additional literature is available to help verify the business entity's legitimacy and the identity of its principals?
- Do legal records demonstrate compliance with local laws, solvency, and the absence of an unfavorable or troubled operating history?

Answering those questions is not always straightforward. For example, "Politically Exposed Persons"—individuals who hold or recently held public positions or perform important public functions, such as senior diplomats, governmental officials, leaders of religious or political organizations, members of ruling royal families, military leaders or judges—are not always identified by global database checks; nor do they always appear in media coverage.

Moreover, a company's websites and other internally generated data cannot replace independent verification of a third party's legitimacy by a skilled investigator. No single source of information can deliver a comprehensive search of international criminal convictions, real estate holdings, or credit reports, and so forth.

Verifying the legitimacy or suitability of a potential partner inevitably requires investigation beyond the validation of self-reported information. So it is wise to engage a reputable professional services firm that possesses the relevant experience conducting third-party due diligence investigations globally.

When your company does enter into a business relationship, compliance managers should ensure that the parties involved understand the anti-corruption laws of the United States, the UK (when relevant), and their home country. In addition, the parties must understand and acknowledge your company's commitment to ethics, compliance, and corruption avoidance. Finally, they must acknowledge that they will act ethically, in compliance with all anti-corruption laws and your company's policies.

No matter where a company has operations, these sorts of warranties and representations have become standard features in any contractual relationship. A written declaration of the third party's intent to uphold anti- corruption and anti-bribery policies and codes of conduct is a fundamental component for due diligence. Many companies find it helpful to automate this process so that due diligence queries, warranties, and representations are systematic and easy to track. Often third parties will sign on to some of the contractual provisions thinking it's a formality and is not material to the contract. It is helpful to have conversations around the contract to ensure anti-corruption and anti-bribery laws are taken seriously.

Diligent

Investigative Tiering

Conducting the investigation of third-party service providers from thousands of miles away is logistically challenging and often impractical. Enlisting a suitably qualified risk advisory firm provides a company with access to the latest compliance-related intelligence, as well as unbiased reporting and expertise in the overseas markets under examination. Engaging an advisory firm that specializes in third-party due diligence also provides regulators with direct evidence of a corporation's commitment to compliance with anti-bribery laws.

Implementing a risk-based approach to vetting third parties and satisfying regulatory expectation generally involves a five-step process:

Step One: Create a Third-Party Inventory

This involves aggregating third-party data from the company's IT systems. First remove duplicates and errors; then determine the type and purpose of each third-party relationship.

Companies often underestimate the number of third parties they have. To capture an accurate third-party inventory, companies must analyze the contents of their ERP and CRM systems, accounts payable records, point-of-sale data, business reviews, interviews, and any other source that may house third-party records. 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. In addition to conducting an initial inventory, companies must also develop a mechanism (ideally automated) that continuously captures newly added third-party relationships.

Step Two: Conduct an Initial Risk Assessment and Classify Third Parties Risk Profiles

In this step, companies determine the general risks that each third party presents. Does the third party operate in a country known to be a high risk for corruption? How much business does it conduct with the company? What percentage of the third party's revenue depends on your business? Does it interact with government officials?

Certain third parties may present greater risk than others. For example, third parties may operate in countries with inherently higher corruption risk than others. That, in turn, warrants increased levels of due diligence. This is important because FCPA compliance requires companies to determine the level of due diligence appropriate for each region where the company engages third parties.

Determining the appropriate level of due diligence includes several considerations. First, a company can consult the latest Transparency International Corruption Perceptions Index to gauge levels of risk for each country in which your business engages third parties. Business conducted in high-risk countries should be vetted to higher standards of due diligence than those typically used in low-risk countries.

The extra steps a company should apply in high-risk countries include:

- A methodical assessment of each third party, in particular those operating independently as resellers, intermediaries, or agents.
- A review of the third party's ownership structure, including whether it is publicly listed on a reputable exchange.
- The manner in which your company engages the third party. For example, if the third party represents your brand in the local market (rather than, say, reselling your products among many others), this presents a higher degree of risk and exposure that justifies enhanced due diligence.

In a similar manner, other types of risk, such as industry-specific risk or business transaction risk impact the process of risk inventory and assessment. Based on that risk calculation, third parties will fall within with a risk profile or tier that has a prescribed scope of due diligence. As an example, high-risk third parties qualify for enhanced due diligence, where a low-risk third party undergoes a global database check (the least in-depth form of analysis).

Step Three: Administer Investigative Due Diligence

When conducting due diligence on a third party, several considerations need attention: the nature of the services delivered, shareholder and management identification, relationships with government officials, the third party's use of its own third parties (that is, your fourth parties), historical compliance issues, conflicts of interest, and the third party's internal control structures.

Companies should investigate high-risk third parties first; this allows you to allocate limited budget to the entities that require the most stringent forms of due diligence. Third parties in the low-risk category can be assessed later in the process. Allocating resources in this manner ensures the most efficient use of time and money; and (based on our knowledge and experience) will be viewed favorably by the DOJ and SEC.

Step Four: Resolve Red Flags

Address red flags or deficiencies identified during the Address red flags or deficiencies identified during the due diligence phase. In certain circumstances, the prudent course of action is to sever ties with a particularly problematic third party, although that is not always necessary. It's often possible to remedy issues with the third party through training, contract revisions, and other steps designed to mitigate risk.

Remember, there is nothing wrong with working with riskier third parties as long as your company takes reasonable extra precautions. A robust and auditable investigation, which includes evidence of a company's efforts to address red flags, helps to demonstrate commitment to anti-bribery compliance.

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. Such mechanisms require proper access given to relevant levels of management and compliance personnel so that they can make informed decisions.

Step Five: Commit to Ongoing Monitoring

The scope of a third-party relationship and the corresponding level of compliance risk it presents are not static. The inherent risk that each third party brings a company can change over time. Reviewing the entire population on a frequent basis helps ensure that the company maintains its understanding of the compliance risk that it accepts and manages within its operations.

Beyond regular review of the company's third-party risk profile, it is critical to respond and make changes if needed both in the compliance program and with respect to a specific third-party. Regulators have made it abundantly clear, and reiterated in the DOJ's 2020 and FCPA Resource Guides, that to have a credible and defensible program a company must also demonstrate how it is learning from mistakes, how it responds to changes related to what it learns about a third-party and the consistency of application of the policies.

Diligent

Investigative Framework

The best way to limit your company's exposure is to treat a third party's past behavior as an indicator of its future behavior. Typically, a risk advisory firm will conduct an investigation based on the following parameters:

- The applicable laws within each country with respect to how data is gathered and used.
- The cultural norms and nuances of professional relationships as well as the country's customs.
- The constraints of local language and political sensitivities.

The depth and scope of each investigation depends on several factors, including the type of relationship under consideration and the inherent risk of bribery and corruption in the third-party's market.

Any due diligence effort should seek to uncover facts, as opposed to merely validating self-reported information. Most companies and individuals in the business of deception will be prepared to provide a portfolio of stories, references, and documents that upon first glance appear legitimate. A trained investigator, with local resources, in-depth knowledge gathered from prior investigations, and access to numerous reliable data sources will uncover inconsistencies that may not appear obvious to the layperson.

The Due Diligence Vetting Checklist

Third-party vetting typically includes the following steps:

- An on-site visit to validate the legitimacy of the company's business operations.
- Examination of corporate records, including the investigation of previous corporate misconduct, litigation, and unreported government supervision or compliance actions.
- An in-depth analysis of the network of business partnerships or affiliations, including the reputation of the company and its principals.
- Criminal background checks performed using appropriate law enforcement resources and publicly available records.
- The third party's financial performance to date, including an understanding of the current sources of funding and list of significant clients.s.
- A review of English language and local press to determine the company's business reputation, major business activities, and other notable social and business relationships. This exercise typically includes reviewing local business reports and professional journals, industry, and mainstream media. Special emphasis is placed on identifying relationships with governmental or political figures
- Existing or prior regulatory concerns associated with local laws and regulations.
- At the conclusion, consideration of whether the subject fully cooperated and provided relevant disclosures when requested.

A company's due diligence effort should also evaluate a third-party's business practices and connection to local government:

- Without violating data privacy laws, ascertain the principals' social and personal relationships with government officials.
- Have any of the third party's principals held political office or served as an official in a political party?
- What service or products will the third party provide? Is the agreed upon compensation commensurate with market rates? What evidence exists to show that the third party is qualified to deliver those services or products?
- How will the third party receive payment? Did the third party designate a bank account housed domestically or offshore? Are payments to be issued in the name of the corporation or some other individual? Will any portion of payment be in cash or a cash equivalent?
- During the due diligence process, have any unusual payment patterns or financial arrangements emerged?
- Has the third party committed to financial transparency and ongoing disclosure of timely and accurate accounting records? Has the third party explicitly acknowledged and agreed

Diligent

to a right-to-audit clause within the vendor agreement?

- Did the due diligence effort confirm the company's place of business and verify that the staffing is proportionate to the remuneration for services to be rendered?
- What does the third party's training on anti-bribery compliance program look like?

Critical Components of Automated Due Diligence

As this paper shows, effective due diligence is a complex undertaking. Although one tool cannot capture the entire analysis and monitoring needed for a comprehensive program, companies should look for a technology platform that automates major aspects of the process. Any program should include standard operating procedures such as:

- Automated issuance of a standardized due diligence intake questionnaire for current and prospective third parties to complete.
- Automated issuance of your company's anti-bribery policy, plus an accompanying anti-bribery agreement letter to be signed by current or prospective third parties.
- Review of a "no fly list" to ensure that a prospective third party has not previously been associated with corruption related activities.
- Selection of the appropriate tier of due diligence based on a review that analyzes inherent risk based on the type of business, geography, and other appropriate factors.
- Structured analysis of resulting red flags, and a defined process to assess the risk in establishing a relationship with the third party under review.
- Automated issuance of third-party agreements, including the integration of relevant audit rights, warranties and representations.
- Retention of all supporting documentation in a secure, encrypted archive. That archive, in turn, should support the following activities:
- Review of due diligence-related metrics, such as caseloads by departments, regional investigative activity, investigation timelines, and volume of completed reports by investigator.
- Chain-of-custody data, including dated and time-stamped records, that documents a commitment to compliance should your program come under scrutiny by regulators.
- Automated notification process to alert third parties for recertification and reaffirmation of the company's commitment to compliance with anti-bribery laws.

Building a credible and defensible third-party due diligence and management program is vital for ensuring compliance with anti-corruption statues. This multi-pronged effort must align an organization's people, processes, and technology in order to prevent and detect violations. Diligent's integrated, risk management solution is the perfect combination of data, insights, technology, and people. Diligent offers configurable compliance solutions that help businesses to thoroughly evaluate and mitigate potential risk.

Resources:

[1] **A Resource Guide to the U.S. Foreign Corrupt Practices Act Second Edition, p. 62**.

[2] **A Resource Guide to the U.S. Foreign Corrupt Practices Act Second Edition, p. 58**.