Deloitte.

International Third-Party Due Diligence
How Much is Enough?

International Due Diligence

Conducting due diligence on international third parties is now considered a leading practice for companies operating in international jurisdictions. Laws such as the US Foreign Corrupt Practices Act (FCPA), UK Bribery Act and guidance from multinational organizations all advise companies to "know" their foreign counterparts. While the need is clear, there is no regulatory guidance specifying a minimum level of due diligence to be conducted. This ambiguity can make it tempting for companies to take a cursory swipe at due diligence; review one database, check the "all-clear" box, and enter into a business agreement.

As evidenced by US Securities and Exchange Commission (SEC) and US Department of Justice (DOJ) judgments in which US companies have been faulted for not performing sufficient due diligence, a cursory approach will no longer suffice. Increasingly, companies are expected to conduct a deeper, more systematic assessment of potential international business agents and partners that involves collecting information from the business partner, verifying the data, and following up on identified "red flags. " This article reviews regulatory guidance on the sufficiency of background research, explores options for information-gathering, and provides factors to consider in the due diligence process.

Guidance on due diligence from the US Department of Justice

The DOJ's Criminal Division published updated guidance in April 2019[1] discussing the factors prosecutors should use to determine whether a company under investigation will be considered to have an effective compliance program. In it, the DOJ reiterates its expectation that an effective compliance program should apply "risk-based due diligence to its third-party relationships."

The guidance acknowledges that while "the degree of appropriate due diligence may vary," prosecutors should nevertheless assess the extent to which the company has an understanding of the "qualifications and associations of third-party partners" as well as the "third-party partners' reputations and relationships, if any, with foreign officials." The DOJ also expects prosecutors to assess whether the company "engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party."

Comments on due diligence in SEC and DOJ FCPA enforcement actions

In addition to this published guidance, actions filed by the SEC and DOJ reveal some common due diligence pitfalls that should be considered when designing an effective compliance program.

Failing to conduct timely and sufficient due diligence

Many companies fail to collect sufficient information on their overseas third parties, and to conduct due diligence in a timely manner. SEC and DOJ enforcement actions have cited situations where companies engaged third parties and conducted due diligence after the fact. In one case,[2] the DOJ faulted a company for hiring a Taiwanese consultant and only obtaining a profile, which indicated the consultant had no relevant experience, two years after the fact. In another case, court papers state that the company "did not conduct any formal due diligence regarding the agent's background, qualifications, other employment, or relationships with foreign government officials before or after engaging him."[3]

The US government has faulted companies for not going far enough in the due diligence process. In one case,[4] the DOJ noted that the company had historically "performed only limited, informal due diligence before retaining third-party sales agents." In another, the DOJ noted that due diligence on an agent was "limited to collecting the company's registration documents, corporate by-laws, and board minutes from agent C himself..."[5]. And in another, prosecutors alleged that the company failed to establish effective due diligence "such as appropriately understanding a given third party's ownership and qualifications, evaluating the business justification for the third party's retention in the first instance, and establishing and implementing adequate screening of third parties for derogatory information."[6]

1 US Department of Justice Criminal Division Evaluation of Corporate Compliance Programs (Updated April 2019)
2 US v. Alcatel-Lucent Trade Int 'I, A.G.
3 US v. Titan Corp.
4 US v. Panasonic Avionics Corporation
5 US v. Embraer
6 US v. Weatherford International Ltd.

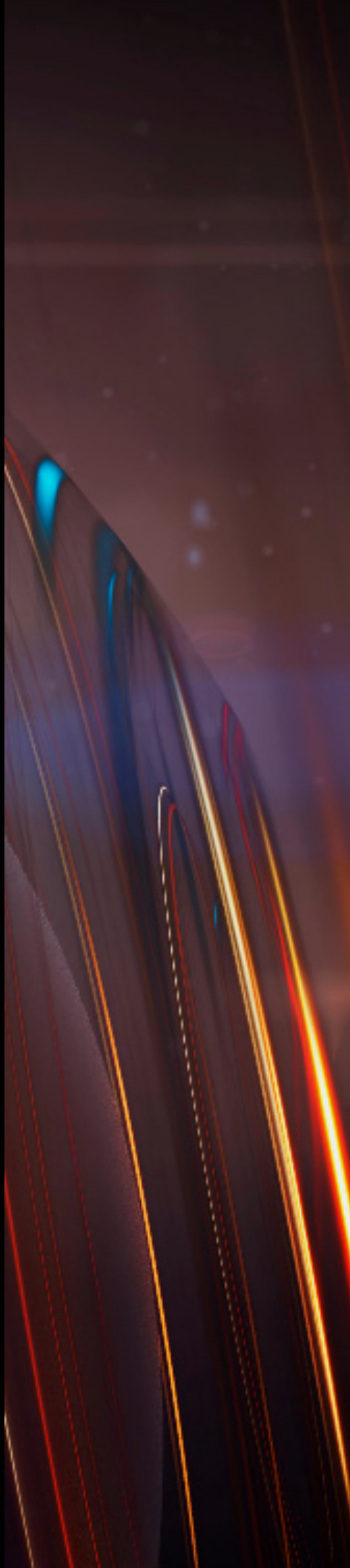
Failing to adequately verify information provided by third parties

Verifying information disclosed on questionnaires completed by third parties is a critical step; numerous SEC and DOJ enforcement actions have criticized companies for failing to do so. In one case resulting from an enforcement action,[7] company officials prepared an internal approval document for a proposed agent in the United Kingdom which "contained false statements as to, among other things, the UK Agent's place of business (falsely stated to be Monaco) and number of employees (falsely stated to be four)." The document was signed for approval by senior company officials, yet "none of the senior [Company A] or [Company B] officials who signed the document undertook any independent review or asked any questions concerning the UK agent."

In a previously cited case[8] that resulted in an enforcement action, the DOJ stated that a company official would typically request a Dun & Bradstreet profile after receiving internal documentation on a potential third party and noted that the company official "made no effort, or virtually no effort, to verify the information provided by the consultant in the Consultant Profile, apart from using Dun & Bradstreet reports to confirm the consultant's existence and physical address." In a previously cited case[9], the SEC noted that the company's attorneys knew that shareholders of a Gibraltar shell company that had received payments were held by two other offshore entities, yet the attorneys "never learned the identity of the beneficial owner[s] of the shares."

Failing to act on identified red flags

The DOJ has also opined on the need for companies to act on risk factors identified during the due diligence process. In a case cited above[10], the DOJ faulted a company for failing to follow up on what were considered obvious red flags identified when hiring a consultant in Honduras for work in the telecommunications industry. As stated in the case, the consultant's company profile, signed by the consultant and the US company's area president, listed the consultant's main business as the distribution of "fine fragrances and cosmetics in the Honduran market" and the Dun & Bradstreet report on the consultant stated that the company was "engaged in cosmetic sales, house-to house." The same case further states that "there was no requirement for the provision of information regarding conflicts of interest or relationships with government officials" and that "even where the Dun & Bradstreet report disclosed problems, inconsistencies, or red flags, typically nothing was done."



7 SEC v. Halliburton Company and KBR, Inc.
8 US v. Alcatel-Lucent Trade Int 'I, A.G.
9 SEC v. Halliburton Company and KBR, Inc.
10 US v. Alcatel-Lucent Trade Int'I, A.G.

Approaching Due Diligence

While there is no law or regulation specifically defining what is "sufficient" international due diligence, the guidance and examples of enforcement actions discussed above do provide some indication of leading practices. Generally, companies can consider several steps in their investigation of a potential int'l 3rd party, including:

- Require the third party to disclose information on a questionnaire.
- Use a risk-based approach to verify the information provided and independently identify adverse information.
- Take action on any identified "red flags" uncovered in the process.

Information disclosure

Companies should design an effective and thorough questionnaire that asks reasonable questions and puts the third party "on the record" regarding certain specific issues. Such a questionnaire should be designed in conjunction with legal counsel and may contain, at a minimum, the following elements:

Company background, including identifying and registration information

Ownership and management, including beneficial owners and others able to exercise influence over the entity and any relationships with government officials, as well as identifying information on these individuals

Disclosure of any civil, criminal, and regulatory matters,to identify a history of issues that may present risk factors

Anti-corruption knowledge and compliance, including questions about knowledge of laws and the company's compliance regime and training efforts

References for individuals knowledgeable about the third party who can provide verification of business relationships and experience

Signature of a responsible party who attests to the veracity of the information and agrees to abide by all applicable laws and policies of the company in carrying out its activities.

Background research methodology

Once the above information is collected, the company should conduct an assessment to determine the level of risk presented by each third party. A number of factors should be considered, including the type of relationship, corruption risk associated with the jurisdiction, interaction with government officials, compliance regime, and known adverse information about the third party. These factors may also vary depending on the industry in which the third party is operating.

Third parties typically are divided into three categories: high-, medium-, and low-risk. High-risk third parties include those located in a country with a considerable risk of corruption, those having significant interaction with government officials, or those for which red flags have been identified in the due diligence process. Medium-risk third parties are those that may have a lesser degree of contact with government officials, such as lawyers or accountants, yet are located in a high-risk jurisdiction. Low-risk third parties might include vendors of goods and services that are not acting in an official capacity for the company.

The methodology for third-party background research will depend on the subject's risk ranking. Figure 1 shows examples of the factors involved in the risk-ranking process and three representative levels of background checks commensurate with those risk levels.

Companies should strongly consider hiring an outside firm to conduct background research to benefit from access to sources otherwise not available and to demonstrate independence in the vetting process. When vetting a representative who has a high degree of contact with government officials, or one located in a high-risk jurisdiction, single-database resources will likely be to be insufficient. Similarly, public record resources in many countries may be to be sparse and unreliable; instead, local resources may be required for record retrieval and for human source inquiries regarding the reputation and background of the subject. Professional investigators may help lower the risk of overlooking important information and provide credibility that the approval process was conducted independently of commercial interests.

What do you need to know about your third parties?

Effective international business partner due diligence requires that a company gather meaningful information, assess potential risk across the enterprise, and tailor risk mitigation actions accordingly. Among key questions a company should ask regarding international business partners:

- Is this a "real" business partner with a business profile and is it experienced in the relevant industry?
- Is the business partner owned by company employees, or do other potential conflicts of interest exist?
- Does the business partner, or its principals, have a track record of bankruptcy or solvency issues that might threaten the supply chain?
- Does the business partner, or its principals, have a history of serial litigation, criminal problems, counterfeiting, child labor, or product safety issues?
- Is the business partner associated with organized crime, terrorist groups, money laundering, bribery, or corruption?
- Is the business partner located in a country restricted by US law from receiving payment, or does the vendor appear on sanction and embargo lists such as that of the US Department of the Treasury's Office of Foreign Assets Control (OFAC)?

Figure 1

[PEP: Politically Exposed Person]
[CPI: The Corruption Perception Index compiled by Transparency International]

Following up on red flags

Finally, where the process does identify red flags, the company should perform additional diligence. As referenced above, when companies have been put on alert by adverse or conflicting information, regulators expect resolution.

In many cases, resolving red flag issues may be as simple as an inquiry with the third party for clarification. For example, if a company self-discloses involvement in litigation, the company may want to inquire about the nature and status of the cases to determine the risk issues.

Likewise, where public record research conflicts with that provided in questionnaire responses, companies may need to make further inquiries with the third party or hire an outside investigator to conduct thorough public record research and source inquiries. In all cases, however, the company should resolve issues and take appropriate steps to assure that they are conducting business with reputable individuals and organizations and document these efforts.

Conclusion

While the due diligence effort may lengthen the start-up time for a new third party relationship, recent SEC and DOJ judgments have demonstrated that failing to do so can have considerable negative financial and operational repercussions for companies seeking to conduct business internationally. It is far better to proceed slowly, carefully, and thoroughly with any new business relationship.

Contact us

Jessica Raskin
Managing Director
Deloitte Financial Advisory Services LLP
jraskin@deloitte.com
+1 212 436 6544

Deloitte.