COSMOS
Navigate the Compliance Universe

CEP Magazine - February 2024

Patrick Wellens (patrickwellens@hotmail.com) is currently working as a Compliance Manager for a division of a multinational pharma company based in Zurich, Switzerland. He is the Vice-Chair of Ethics and Compliance Switzerland, co-chair of the working groups "life science" and "anti-corruption," and Head of Governance of the Association of Corporate Investigators.

Third-party due diligence: Are supplier questionnaire(s) the answer?

By Patrick Wellens, CCEP-I, CIA, CFE, CRMA, MBA

Numerous laws (U.K. Bribery Act guidance document,[1] German Supply Chain Act,[2] Foreign Corrupt Practices Act resource guide,[3] *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas*,[4] French vigilance law,[5] U.K.'s Modern Slavery Act,[6] EU's Corporate Sustainability Directive[7]) require companies to *conduct due diligence* in their supply chains to prevent forced labor, child labor, violations of human rights, or prevent corruption in third parties. Also, when outsourcing certain data-processing activities to third parties, the company must make sure that these parties abide by General Data Protection Regulation standards and, hence, must conduct some due diligence to ensure this is the case.

Companies can do an initial risk assessment of these third parties and, based on each risk domain (corruption, human rights, sustainability, IT security, data privacy), define methodologies to create "low," "medium," or "high-risk" third parties. The higher the inherent risk, the more due diligence is needed.

None of the previously mentioned laws explicitly define what documents need to be reviewed as part of due diligence. The following evaluates the various scenarios companies could apply to conduct (enhanced) due diligence.

Due diligence scenarios

The aim of conducting due diligence is to prevent reputational risks and fines by working with third parties that abide by the company's supplier code of conduct, laws, and regulations. What options do companies have to conduct due diligence? In the case of third parties with medium or high risk, the company could select from the following options.

Option 1

A company sends out a questionnaire to a third party and asks the third party to provide some information.

Depending on the risk domain (corruption, sustainability, data privacy) being evaluated, the questions sent to the third party/supplier will be different. The questionnaire can request the third party to provide information about the length of the business relationship with your company, whether the they have had any other company name in the last 10 years, who the ultimate beneficial owner or main shareholders are, whether the management of the company contains any politically exposed persons, whether the company has been involved the last five

years in any criminal investigations, etc. In addition, the third party might also be asked to provide certain evidence to support the answers given in the questionnaire. The third party might have to upload evidence that they have an anti-corruption policy, a policy on sustainability, a data privacy policy, or an International Organization for Standardization (ISO) certification.

Where the answers provided by the third party are not corroborated with any other data, there is little assurance that the answers are correct. In such scenarios, the company almost entirely relies on the honesty of the answers provided by the third party. If, on the other hand, the external third party supports answers by providing evidence, then the assurance of honesty is higher.

Option 2

A company does not use questionnaires but relies on the third party's certification.

A company does not conduct due diligence on the supplier because the supplier has an ISO 37301 (compliance management system) or 37001 (anti-bribery and corruption) certification or has gone through an EcoVadis sustainability assessment.

Option 3

A company does not use questionnaires but uses external data sources.

On the market, there are numerous research and data providers that companies can use to screen a company and/or its directors against sanction lists, law enforcement or terrorist lists, or adverse media (e.g., whether a company was ever involved in or was convicted for money laundering, tax evasion, antitrust violations, child labor violations).

Whereas some data providers specialize in particular risk domains, they might not be strong in others. A company that is highly specialized in IT security data points (for instance, BitSight) might not have a large database on human rights, environmental, corruption, or regulatory news.

Given that most of the data providers have research analysts in almost all countries and regularly screen the press and add articles to their databases, the external data sources are of course more independent and possibly more reliable than the answers given by companies in the questionnaires. However, if a company does not come up in the news for corruption, money laundering, and/or tax evasion, it does not mean the third party has a robust compliance program that prevents such corruption cases from happening.

A disadvantage of using external data to conduct due diligence is that each screening of a third party against the database costs money. Screening each third party for a multinational company with 100,000 suppliers and 10,000 commercial third parties (e.g., distributors, wholesalers, resellers, sales agents) is not realistic or recommended.

Option 4

A company uses questionnaires and external databases.

Using a combination of external databases and questionnaires covers more ground. External databases allow the company to evaluate the third party's reputation by screening the company name, main shareholders, ultimate beneficial owners, or main directors against sanctions and adverse media lists. At the same time, the questionnaire evaluates the effectiveness and validity of a company's claims about its policies and training to mitigate risk.

Option 5

In addition to Option 3 or Option 4, the local compliance officers are involved in conducting due diligence.

A compliance officer in countries where a new, high-risk third party will be selected could reach out to fellow local compliance officers and inquire about the reputation of the third party and/or conduct additional due diligence activities (e.g., verification of documents at local courts).

Option 6

Enhanced due diligence by an external service provider in combination with Options 1–4.

Prior to selecting a new high-risk third party—usually in countries or emerging markets where the company does not have a presence—companies might use the services of external parties to conduct so-called "enhanced due diligence." The external companies offering such services would then verify whether the third party indeed exists at the given address and inquire in the local market about the third party's reputation by talking to customers or suppliers. Option 6 might be very useful for high-risk transactions.

Even though external providers might conduct due diligence activities more efficiently than if they were conducted in house, it is important to highlight that the legal obligation to conduct proper due diligence cannot be delegated to external providers but remains with the company that engages the third parties.