Conducting Effective and Ethical Anti-Corruption Risk Assessments

Mark Morrison, Blake, Cassels & Graydon LLP
Jon Drimmer, Paul Hastings LLP

PAUL HASTINGS | Blakes

Why Conduct a Risk Assessment?

Anti-bribery and corruption (ABC) risk assessments are among the most important components of a compliance program. In April 2019, the United States Department of Justice (DOJ) published a guidance document entitled *Evaluation of Corporate Compliance Programs* (Guidance) to assist prosecutors in evaluating the effectiveness of ABC compliance programs when making decisions related to enforcement, resolution, penalties and continuing compliance obligations related to misconduct. According to the Guidance, using risk assessments to tailor ABC compliance programs is fundamental to receiving credit from the DOJ:

> The starting point for a prosecutor's evaluation of whether a company has a well designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.

The Guidance also states that an ABC compliance program that focuses resources on high-risk areas may still receive credit, even if it failed to prevent misconduct in a low-risk area.

The Guidance makes clear that the DOJ expects companies to determine their risk profiles, and tailor their ABC compliance programs pursuant to these risks. Risk assessments are the most effective tool to fulfil this requirement.

Initial Considerations

Conducting effective assessments can be challenging. It is important that assessments are well planned, effectively scoped and tailored to reflect the specific businesses or operations being assessed.

There are some important considerations to be had before conducting a risk assessment. For example, ABC risk assessments require specialized expertise and knowledge. In light of the potential sensitivity of findings, it is also prudent to structure risk assessments in a way that maximizes potential privilege protections. As such, legal counsel with risk assessment expertise should be involved at all stages of the risk assessment, including the development, oversight and execution stages. In addition, a risk assessment must maintain sufficient independence from internal pressures to be a credible analysis of a company's risks.

When Should a Risk Assessment Be Conducted?

Risk assessments should be conducted both early and periodically. While risk assessments are a critical first step in developing a strong and effective compliance program, they are also important for periodically testing how a compliance program is working while identifying new developments and changes. Regardless of the maturity of a compliance program, risk assessments are important.

Companies may also conduct risk assessments when they are considering a major acquisition or entering into a business area or market to better understand the corruption-related risks associated with those plans before moving forward.

Risk assessments are not a one-and-done exercise. Multinational companies are expected to regularly review their operations, asses their risks, test the effectiveness of their compliance programs, and adjust and enhance their controls as necessary.

Can a Company Use a Generic Risk Assessment?

There is no one-size-fits-all risk assessment. To be most effective, risk assessments should focus on areas identified as potentially exposed to a higher risk of corruption. The DOJ and SEC have explained that "[o]ne-size-fits-all compliance programs are generally ill-conceived and ineffective because resources inevitably are spread too thin, with too much focus on low-risk markets and transactions to the detriment of high-risk areas."

While there is no one-size-fits-all risk assessment, risk assessments usually follow similar stages: planning, execution, analysis, reporting and responding to identified risks.

What Kind of Corruption Risks Does a Risk Assessment Review?

An effective risk assessment will identify and prioritize potential corruption risks in a company's operations, identify and assess the effectiveness of a company's existing controls in addressing those risks and make recommendations to address any potential gaps between identified risks and existing controls.

General corruption risks facing a company include the inherent risk of corruption associated with jurisdictions, industries and regulatory environments in which it operates. After evaluating these general corruption risks, a risk assessment should examine specific areas of risk facing the company based on touch-points with government that can include, but are not limited to: its compliance history; its partnerships and joint ventures with third parties, including government; its interactions with regulators for licenses, permits or leases; expenses related to hospitality, entertainment, gifts, charitable contributions, political contributions or lobbying; recent mergers and acquisitions; employees connected to government; and whether the company uses third-party representatives to act on its behalf. These specific areas of risk should be tailored to the business of the company.

Reviewing the effectiveness of existing ABC controls includes a consideration of:

- Existing policies, procedures and internal controls in place and their effectiveness
- The level of oversight and involvement of senior management in ABC efforts
- The infrastructure in place to provide ABC training to the employees and what the training covers

- The confidential reporting, anti-retaliation and investigations apparatus of the company
- Incentives and disciplinary measures in place
- Monitoring, auditing and other financial internal controls related to the prevention or detection of corruption
- Reporting obligations throughout the organization, with an understanding of the nature of decision-making authority and oversight controls

Planning and Conducting a Risk Assessment

Early in the process, it is important to identify the scope of the risk assessment and determine the methodology for collecting and analyzing the information. A risk assessment should typically include a desktop review, documentary reviews, interviews and reporting.

Desktop (Baseline) Review

The first step of a risk assessment typically includes a desktop, or baseline, review. This step involves undertaking a general overview of the corruption risks facing the company and will help with identifying the operations and functional areas that deserve a greater compliance focus. The desktop review involves a general review of the country risk, the sector risk and the nature of the business.

- **Country Risk:** This step involves a review of the corruption risk in the countries where the company conducts business. The company's exposure risk increases in jurisdictions where there is perceived to be a higher rate of corruption. Compliance resources should be prioritized for countries where bribery and corruption are perceived to be most prevalent.
- **The Sector Risk:** Some sectors are perceived to have higher risks than others, based on reputation and other factors. These sectors will be more closely scrutinized by regulators.
- **The Nature of the Business:** Different businesses have different risk exposures. For example, the more extensive the contacts with government officials, and the more important the interactions are to the company, the greater the risk of corruption. This also means that a risk assessment must consider if the business has many different stages of development that require government interaction, such as license approvals or sales. Finally, corruption risk will increase as a company's central control of a business asset or operations decreases and the control of partners, including joint venture and government partners, increases.

In addition to the above, the desktop review may identify other risks such as whether the company has newly acquired businesses or whether the company (or similarly situated companies) have faced corruption allegations or charges in the past. These would both increase the risk facing a company.

At the end of the desktop review, a scorecard can be created assessing the company's overall risk profile. The scorecard can then be used to assist with tailoring the risk assessment moving forward and provide an initial basis for knowing which documents should be reviewed.

> **Practical Tip:** A scorecard is a simple but effective means of demonstrating the product of an initial assessment exercise.

Documentary Reviews

Once the initial desktop review has been completed, targeted document requests can be made and the documents reviewed. The objectives of documentary reviews are to:

- Review relevant policies and procedures
- Learn how policies and procedures work in practice
- Review relevant internal audit reports and the results of other assessments and inquiries.

The documentary review should also include a sampling of certain transaction and due diligence documents such as receipts or invoices, internal approval materials for payment requests, agreements and memoranda of understanding, rosters of individuals, vendors and employee onboarding files, and other documents in the areas being assessed.

The documentary review will help shape and focus the assessments, or lead to additional questions or interviews, and are considered in the overall analysis of the information gathered during the assessments.

Questionnaires

Questionnaires are an efficient tool to collect information on corruption risks from employees throughout the company. Questionnaires are particularly effective for risk identification for companies with different locations and operating units. In addition, questionnaires can help with determining the appropriate employees to interview. The questionnaires provide a customized set of corruption risks driven largely by knowledge, attitude and processes of the specific part of the company's operating environment.

Practical Tip: Questionnaires should be written in plain language, understandable by a work force and tailored to the job function of the person responding.

Interviews

Most of the risk-assessment testing phase involves in-person interviews designed to obtain first-hand knowledge from a diverse group of employees at different levels about their perceptions of the greatest risk areas they perceive in the company's operations. These interviews will also seek to identify the nature, frequency, importance and extent of government interactions, and the government officials and agencies wit h which those interactions occur.

Before substantive interviews are conducted, a mapping exercise should be undertaken to determine the appropriate personnel who will participate in the interviews. It is important to interview not only management, but also those responsible for the day-to-day activities of the business and, specifically, gatekeepers and those who directly or indirectly engage with government. These employees are the ones who have the first-hand experiences and perceptions of the risks the company faces.

In addition, the interviews are designed to identify and evaluate:

- The strength of anti-bribery and other relevant processes and controls, including the familiarity of relevant personnel and gatekeepers with those processes and controls and how closely they are followed
- The effectiveness of training and reporting mechanisms within the company
- The culture of compliance within the company and tone from the top
- The strength of related internal financial controls, including how payments involving government are booked, the availability and nature of backup documentations, and the degree to which delegation of authorities are followed

Conducting interviews in person is preferred, although when necessary, telephone interviews may be appropriate.

Reporting

Following the interview and document assessment phase, a report should be prepared identifying, on a risk-weighted basis, the risks the business faces from an ABC standpoint. The report should identify the controls that address these risks and any gaps between risks and controls, as well as make recommendations to address any such gaps.

Practical Tips:

- Effective reports are to the point, not unduly lengthy and have a risk-rating system consistent with how the company reports in other risk analyses. For instance, if the company uses "stoplights" to reflect risks, use stoplights; if the company has a numerical risk rating, considering using that approach.

- Recommendations should be practical and achievable. Making impractical recommendations can set up the organization for failure. Therefore, reviewing draft recommendations with company personnel with responsibility for implementation in advance of finalization is best practice (both from the perspective of ensuring workability of recommendations and because company personnel can also offer valuable practical implementation insights and suggestions).

Simply identifying ABC risks is only the first step. Companies must then evaluate and remediate any weaknesses identified in the risk assessment. While a company cannot do everything at once, regulatory authorities expect companies to make legitimate attempts to develop and execute remediation plans to address issues and concerns identified in the risk assessment.

The DOJ and SEC have affirmed that they 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.

Practical Tip: Remediation plans should identify the task, the person responsible and the deadline. In general, unless there is a substantial finding, remediation deadlines should be completed within six months.