TRACE

A Guide to Corruption Risk Assessment and Risk Mapping

Introduction

All major transnational anti-corruption laws require—or at least presuppose—risk-based compliance programs. In their Resource Guide to the Foreign Corrupt Practices Act, the U.S. Department of Justice (DOJ) and Securities and Exchange Commission (SEC) state:

> *Assessment of risk is fundamental to developing a strong compliance program, and is another factor DOJ and SEC evaluate when assessing a company's compliance program. One-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. Devoting a disproportionate amount of time policing modest entertainment and gift-giving instead of focusing on large government bids, questionable payments to third-party consultants, or excessive discounts to resellers and distributors may indicate that a company's compliance program is ineffective.*[1]

Similarly, the UK Ministry of Justice (UKMOJ) identified risk assessments as a key principle of compliance programs in its Guidance to the UK Bribery Act, stating that "adequate bribery prevention procedures ought to be proportionate to the bribery risks that the organisation faces. An initial assessment of risk across the organisation is therefore a necessary first step."[2]

France's Sapin II law expressly requires subject companies to conduct "risk mapping in the form of regularly updated documentation designed to identify, analyze and prioritize risks of the company's exposure to external solicitations of corruption, in particular by taking into account the industry sector and the location of company operations" and to undertake due diligence on their customers, first-tier suppliers and intermediaries based on the results of such risk mapping. [3]

No One-Size-Fits-All Approach

As there are no effective one-size-fits-all compliance programs, there is no standard risk assessment or risk mapping process for all companies and scenarios. The French Anticorruption Agency (AFA) has put it simply: "Each company draws up its own risk mapping specific to it, and therefore it cannot be applied as it stands to another company."[4]

Although there is no single recipe for risk assessment, government agencies in the United States, the UK and France have put out general guidelines and even prescriptive steps (in the case of the AFA) regarding risk assessment/mapping and methodology.

United States

In evaluating the effectiveness of corporate compliance programs, the DOJ examines "whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations."[5] The DOJ also focuses on documented risk assessment methodology, relevant information-gathering and data access, metrics used, periodic updates to risk assessments, and the incorporation of any lessons learned from the company's own prior missteps or those by other companies operating in the same industry or geographical region.

UK

The UKMOJ's 2011 Guidance indicated that risk assessment should be "periodic, informed and documented."[6] Risk assessment procedures should be "proportionate to the organisation's size and structure and to the nature, scale and location of its activities." Among factors affecting the company risk profile and compliance approach, the UKMOJ listed the size of the organization, the nature and complexity of its business, and the type and nature of associated persons (i.e. third parties). More specifically, the UKMOJ called on companies to analyze the following external risk factors:

- **Country risk.** Higher-risk countries include those with high levels of perceived corruption; lack of effective anti-corruption laws; and ineffective anti-corruption efforts by the local government, the media, the business community and civil society.
- **Sectoral risk.** Some industries, such as the extractive and large-scale infrastructure sectors, are exposed to higher corruption risks.
- **Transactional risk.** Some types of transactions are associated with higher corruption risks, e.g. charitable or political contributions, government licenses and permits, and public procurement transactions.
- **Business opportunity risk.** High-value projects, projects with numerous contractors or intermediaries, projects at prices not commensurate with market rates, or projects without a clear legitimate objective can present opportunities for corruption.
- **Business partnership risk.** Some relationships—such as those that involve the use of intermediaries, transactions with foreign public officials, state-owned or -controlled companies, consortia or joint ventures, or relationships with or linked to Politically Exposed Persons—can lead to higher corruption risks.

The UKMOJ also listed the following internal risk factors that may need to be analyzed as part of a risk assessment:

- deficiencies in employee training, skills and knowledge;
- bonus culture that rewards excessive risk taking;
- lack of clarity around the organization's policies on/procedures for hospitality and promotional expenditure, and political or charitable contributions;
- lack of clear financial controls; and
- lack of a clear anti-bribery message from top-level management.

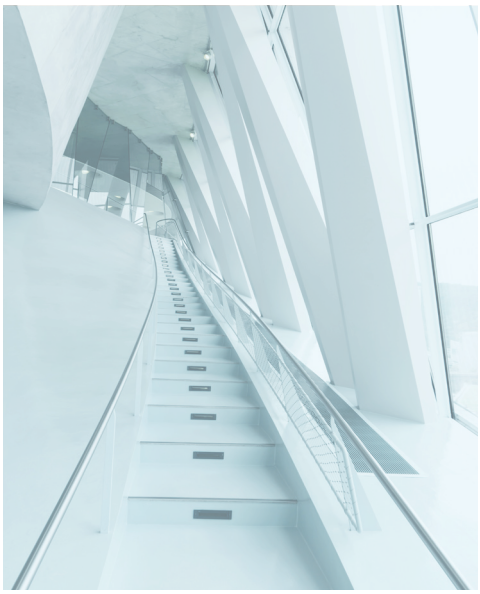
France

In January 2021, the AFA issued its updated guidelines under Sapin II law, devoting six detailed pages to the risk mapping (*cartographie des risques*) process.[7] The AFA explained that the risk mapping exercise should be "objective, structured and documented" and have "due consideration of the specific features of each company, including activity sectors, locations, competition and the regulatory context, types of third parties, business model, value chain, activities and processes, internal organisation of the company, decision-making circuits." The AFA-recommended process seeks to identify all business processes that may lead to any interaction with outside parties, along with all associated inherent corruption risks before and after controls are taken into account. The AFA guidelines specifically discuss "gross risks" (*risques bruts*), the corruption risks to which a company is exposed without regard to any compliance or control measures—and "net or residual risks" (*risques nets ou résiduels*), the corruption risks that remain after taking into account any existing compliance and control measures. The guidelines recommend analyzing these risks in terms of probability (likelihood) of occurring and their degree of impact (severity) on the company in light of any particularized aggravating factors. According to the AFA, the goal of risk mapping is to inventory and rank such processes and risks, allowing company management to effectively mitigate them by drawing up and implementing a well-informed action plan that consists of customized risk-based prevention, detection, and remediation measures and procedures.

The AFA describes in detail six recommended steps of the risk mapping process:

1. roles and responsibilities of risk mapping stakeholders;
2. identification of the risks inherent in the company's activities (process identification and risk scenarios);
3. assessment of gross risks (risques bruts);
4. assessment of net or residual risks;
5. net or residual risk ranking and preparation of the action plan; and
6. formalizing, updating and archiving the risk map.

Information-Gathering Methodology



There are numerous ways to obtain input data for company-specific corruption risk assessment. Companies may circulate custom risk assessment questionnaires to corporate leadership and to different functions within the organization, and possibly external questionnaires to select third parties. It is important to have representation from employees at all levels of key functions throughout the company, including top management, mid-level management and those on the ground who may directly face compliance challenges. The company can also conduct interviews and brainstorming sessions with working groups based on the risk assessment discussion prompts and the analysis of relevant information, legislation, history of internal incidents, enforcement trends, media reports, internal audit and control reports, and the like.

Companies may combine these steps, sending out questionnaires first and organizing working group sessions based on preliminary results. See Appendix A for a collection of sample questions that may help you devise your own risk assessment questionnaires or discussion prompts.

It can be helpful to identify a list of corruption risks in advance as the starting point for questionnaires, interviews and group discussions. It is, however, important not to prejudge the outcome of the risk assessment questionnaire responses or group discussions, and to leave room for open-ended questions to be able to identify new and yet-to-be-uncovered risk scenarios to which the company is exposed in the course of its operations.

Risk assessments should closely review and analyze any compliance incidents within the company and hotline reports over the last 12 to 24 months to identify any patterns, risk areas and lessons learned. It is also expected that companies will review any law enforcement trends or media reports about other companies in the same industry or geographic location facing anti-corruption compliance challenges, conducting internal investigations, or undergoing government investigations or enforcement actions to see if their own company is faced with similar challenges and whether it adequately manages similar risks.

If appropriate, companies may consider using data analytics approaches based on continuous access to operational data and enterprise information. Indeed, when evaluating corporate compliance programs, the DOJ asks the following questions, among others:[8]

- *Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions*?

- *Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?*

Whatever methodology you choose, it should be documented and applied consistently during the risk assessment process so that information obtained from various business lines, subsidiaries and geographic locations can be meaningfully aggregated and analyzed.

Risk Analysis and Quantification

Based on the information collected through questionnaires, interviews and group discussions, identify the corruption risk scenarios facing the company. Each time a corruption risk and its nature are identified, one way to analyze it is to use qualitative "word-based" estimates of risks' likelihood and severity (e.g., likely, unlikely, high, moderate, low, etc.) without assigning any numerical values but supporting such estimates with narrative analyses. Qualitative narrative-based risk assessment may be preferred by those who find it difficult, arbitrary or speculative to settle on one specific number when quantifying risk values. Even when using the quantitative approach discussed below, there should be place for a qualitative common-sense verification of the result to confirm that it makes sense to an experienced compliance professional and that it has not suffered from an Excel input error, lack of foresight in the design of the risk assessment protocol or manipulation of the numerical risk scores.

The French authorities have indicated their preference for a quantitative risk mapping, with the basic formula for quantifying risk being as follows:

Risk = Probability (likelihood) of risk occurring **x Impact** (severity) of risk occurrence **x** any applicable **coefficients** for aggravating or extenuating circumstances.

To make use of this formula in practice:

1. Choose a scale, e.g. from 1 to 5,* for measuring risk probability and impact, with 1 being the lowest and 5 being the highest.

2. Choose the risk boundaries for low, moderate, significant and high risk.** Given that incidents of bribery and corruption violate the law and may lead to significant penalties and prison terms for

*If you find it difficult to differentiate gradations on the 1-to-5 scale, you may use a scale of 1 to 3: low, medium and high.

**As in the preceding footnote, you may decide to limit the risk categories to three: low, medium and high.

those involved, the risk categories are not equally distributed between the four categories but are typically skewed toward higher-risk categories. For example, you may choose to define risk boundaries as follows: low risk from 1.00 to 3.99, moderate risk from 4.00 to 6.00, significant from 6.01 to 10.00, and high risk from 10.01 to 25.00.

Your risk matrix (heat map) may look something like the following example.

PROBABILITY (in the next 12 to 24 months)								
	> 90%	Almost certain	5	5	10	15	20	25
	50-90%	Likely	4	4	8	12	16	20
	20-50%	Possible	3	3	6	9	12	15
	5-20%	Unlikely	2	2	4	6	8	10
	< 5%	Rare	1	1	2	3	4	5
				1	2	3	4	5
				Insignificant	Minor	Moderate	Major	Critical
				IMPACT				

3. The baseline risk numbers—calculated using "the fullest, most suitable information for the specific nature of the identified risk"[9]—may need to be fine-tuned to account for any extenuating or aggravating factors not included in the baseline assessment. For example, operations in the bottom 50 countries on TRACE's Bribery Risk Matrix could introduce a coefficient of 1.5, so that a risk with a baseline probability of 2 and an impact of 5 for a total risk of 10 (i.e. moderate risk) would be converted to a total risk of 15 (i.e. high risk) after applying the 1.5 coefficient. In contrast, operations in the top ten least risky countries on TRACE's Matrix could offer a 0.8 coefficient to reflect the lower expected incidence of business bribery in those countries. Other possible coefficients could be applied in instances of the company's participation in government procurements that do not follow transparent tender procedures, that involve commissioned agents, or that exceed a certain threshold value amount—unless these are treated as separately identified corruption risks.

4. Conduct separate evaluations of each identified risk before any controls (so-called inherent risk assessment), and then take into account any existing controls (so-called residual risk assessment).

5. Group the risks according to their nature and score, and prioritize them, which will result in a classification of risk scenarios by level.

You may consider some of the following factors when evaluating the likelihood of corruption risks occurring:

- the nature of the transaction or process (e.g. need for interaction with government officials or other government touchpoints, a sale of items within an established competitive market and easily identifiable market prices versus procurement of unique high-value systems with no publicly established market prices, provision of hard-to-value-and-document consulting services);
- involvement of third party intermediaries;
- high level of corruption in the country;
- past history of corruption in the industry or the company;
- inadequate compliance culture, lack of management support and resources;
- degree of the applicable regulation and red tape;
- degree of discretionary authority from the customer or government official;
- degree of price transparency and market discipline (e.g. public tenders versus sole-source procurements of unique high-value systems);
- existence—or lack of—transparent, well-established, verifiable government or regulatory processes (e.g. participation in online government tender procurement mechanisms accessible to the public versus a non-transparent sole-source military procurement);
- number and frequency of transactions or interactions with government officials;
- complexity, experience and sophistication required for contract performance (e.g. a company whose high-tech product is an established market leader with few replacement options may have a different risk profile than a company with less-than-competitive low-tech products); and
- number of entities, individuals or steps involved.

When evaluating the risks' overall impact, you may consider the following consequences:

- reputational and brand damage;
- legal and regulatory consequences, such as government enforcement actions, investors' lawsuits, blacklisting by customers, debarment from government procurements, independent compliance monitor;

- financial consequences, including loss of business, potential criminal penalties, costs of internal investigation and legal defense, potential shareholder litigation; and
- other consequences, such as prison sentences for management and employees, loss of employee morale, business disruption, loss of productivity, loss of competitiveness, etc.

Documenting Risks

Once the risks are identified, analyzed and prioritized, it is important to keep a record of all identified risks, their assessments, controls and compliance measures, and any risk management steps. Each risk can be documented separately, or risks can be reflected in a risk register similar to the example below.

Risk	Inherent Risk			Risk Owner(s)/ Business Unit	Existing Controls, Compliance Measures, Mitigation Steps, etc.	Effectiveness	Residual Risk			Assessment Date	Risk Management Action	Target Date
	Impact	Pribability	Total				Impact	Pribability	Total			

Risk Management Action Plan

For risks that are not adequately addressed by the existing compliance program and controls (i.e. those with high residual risk scores), draw up an action plan to adequately address such risks based on their priority, documenting the steps to be taken, action owners, timetable, implementation, monitoring and reporting procedures. This will help establish the company's objective documented risk management strategy.

Conclusion

When conducting a risk assessment, do not lose sight of its objectives. The risk assessment is not the end in itself. Rather, it should inform the company's management of the true corruption risks associated with the company's operations, help evaluate the effectiveness of the existing compliance program and controls, and ultimately allow the company to allocate its compliance resources toward managing the identified risks through prevention, detection and remediation measures proportionate to those risks and adapted to the company's unique risk profile.

APPENDIX A

Sample Risk Assessment Questions

This is a collection of sample questions that you may choose from, omit or expand upon to compile your own risk mapping questionnaire and interview or group discussion prompts specific to your organization, sector and operations. The sample questions below may overlap or even cover the same topic and vary only in their wording or focus. They may also leave gaps in coverage of compliance areas specific to your company.

The questions can be left open-ended, inviting a free-form response; used as prompts in a group discussion; or used to invite respondents to agree or disagree with them on a confidence scale from "strongly agree" to "strongly disagree." The open-ended format is useful to prompt discussion or solicit information that may not otherwise be reported to management. The multiple-choice format is especially useful for statistical analysis of responses, making them uniform, quantifiable and easier to process. Information obtained in response to some of the questions may require follow-up or discussion.

General Background, Compliance Culture, Work Environment, Public Image

- Do employees of our company have a strong sense of responsibility toward the company and its shareholders and seek to protect company's brand and reputation?
- Does our company value integrity, good governance and ethical conduct in the workplace and when pursuing business?
- Do top leaders of our company lead by example in following values of integrity, good governance and transparency?
- Does our company have zero tolerance for corrupt conduct?
- Are employees of our company law-abiding?
- Are you comfortable that our employees will make the right ethical decisions in challenging situations and will know when to seek advice or assistance?
- Are employees of our company honest in their dealings with each other, customers, government officials and outside parties?

- Does our company have a formal enterprise business process management system, formal business process inventory or process map reflecting all main managerial, operational and support business processes? (If so, the risk analysis questions can be organized around the existing process map).
- Does our company have a good compliant corporate culture as a whole?

Our Company's Operations

- Outline with words or draw our company's entire product development and manufacturing cycle, sales cycle, and contract performance cycle. Are there any other complex activities that can be similarly outlined (e.g. regulatory approvals, clinical trials, product launch and marketing promotion, constructing new facilities, mergers and acquisitions)?
- With our company's manufacturing, sales and other cycles as a background, identify any potential interactions with government officials, customers or other outside decisionmakers or
- gatekeepers (e.g. regulatory approvals, technical certification, standard-setting bodies) and any other government touchpoints that our company has either directly through its employees or through anyone who can act on behalf of our company.
- Does our company, along with its business units and departments, establish and follow clear budgets and adequately justify, account for and document spending decisions?
- Are high-value spending decisions centralized or decentralized? How are they approved, processed and documented?
- Are low-value spending decisions centralized or decentralized? How are they approved, processed and documented?
- Does our purchasing department have robust procedures and controls? Do we use vendor vetting, price justification and verification, escalating authority for approving higher-value purchases, or tender or multiple bid requirements for purchases over certain thresholds?

Sales and Marketing

- What are our company's routes to market (the ways our products or services reach ultimate customers or end users)? Explain in detail (e.g. internal sales force, distributors, intermediaries, resellers, etc.).
- Do we sell internationally, directly or indirectly? Explain.
- Do we do business overseas? Are we considering overseas expansion?
- Do we transport our products, services, equipment or staff across borders (even temporarily)?

- Do we sell to government or military customers or government-owned or -controlled enterprises?
- Does our company otherwise derive any revenue directly or indirectly from state budgets or other public sources (e.g. taxation, customs duties, government-mandated fees)?
- Does our company have or seek a preferential or protected position in the market owing to government regulation, license or otherwise? In other words, do we enjoy any government preferences or exemptions (e.g. tax incentives, tax forbearance) that are not available to all market participants? Explain.
- Do we operate in industries or regions where the government has significant ownership or other control over our customers or other relevant economic actors (e.g. China, nuclear energy industry, healthcare in many countries)?
- Do we take steps to influence or help set applicable government or industry standards or technical specifications? Explain.
- What is the typical value of our company's sale? Does our business model include large-scale projects, government tenders or long-term contracts? Do we engage in a large number of small transactions or infrequent high-value transactions?
- How are the prices set for our products and services?
- Do our company's products/services have easily identifiable market prices set by a competitive marketplace?
- Do we have a public price list for our products/services? Are our prices transparent to the marketplace or kept confidential?
- How much do our prices vary from customer to customer or region to region? What are the reasons for any significant variations?
- Is our product/service an established market leader with few real competitors/replacements, part of a very competitive marketplace, or a less-than-competitive offering?
- What is our company's value proposition or what does our sales force focus on when giving a sales pitch to a potential customer? Which of the identified factors could potentially be manipulated or improperly influenced?
- How do we promote and incentivize sales? Do we offer commissions to sales agents? Rebates to customers (retailers, end users)? Bonuses? Samples? Prizes? Raffles? Trips? Paid speaking engagements?
- Does our company sponsor, finance or otherwise cooperate with opinion leaders, research institutes, consumer groups or industry associations to disseminate messages that are beneficial to us among the public or other target audiences? Are any of these target audiences government officials, employees of state-owned enterprises, hospitals, research institutes or universities? Explain.

- Do our products/services need to obtain a government or industry certification/approval before being marketed (e.g. pharmaceutical products, certain medical or industrial equipment, etc.)?
- Do we operate in highly regulated sectors? Explain.
- What permits, licenses, inspections, certifications, tariff classifications, authorizations or approvals is our company required to obtain from government agencies or other bodies?
- Are there laws, regulations, or technical or industry standards that serve as a significant impediment to our business or, on the contrary, significantly benefit our business? What steps, if any, does our company take directly or indirectly to address such impediments or to secure and retain the benefits?
- List any other government touchpoints that our employees or third parties may have on behalf of our company that have not yet been mentioned.
- When interacting with government officials or customers, are our employees or third parties faced with requests for improper payments?
- When interacting with government officials or customers, do our employees or third parties have incentives to offer improper payments or to risk engaging in other misconduct?
- Is the industry in which we operate known for high risk of corrupt conduct?
- Have competitors or other companies in our industry been investigated, prosecuted or mentioned in adverse media reports for corrupt conduct?
- Are we operating in countries where bribes or facilitation payments are a frequent part of doing business? Do we sell, directly or indirectly, in such countries?
- What other business decisions do we face where bribes or facilitation payments are expected?
- If a sales manager does not pursue a prospect or stops a large sale over serious compliance concerns that hurts our company's bottom line, what are the potential personal consequences to this manager? What would be the impact on his annual performance evaluation and compensation?

Third Parties

- What outside parties (e.g. intermediaries, consultants, suppliers, advisors, distributors, resellers, marketing representatives, joint venture/teaming arrangement partners, lawyers, accountants, freight forwarders, media buying agencies, other third parties) are typically used during the product and sale cycles outlined above?
- Which of these third parties interact with government entities or customers on behalf of our company?

- Does our company ever retain the services of outside parties (lawyers, tax advisors, consultants, freight forwarders, transportation companies, "fixers") to interface with government officials or employees on behalf of our company?
- Even if our company does not pay and has no direct contract with such third parties, does anyone else (e.g. third parties retained by our intermediaries, consultants, lawyers, freight forwarders, etc.) interface with government officials or employees in connection (however remote) with the sales, transportation or promotion of our products/services?
- How do we compensate outside parties? For example, do we offer success fees, sales commissions, discounts, extra bonuses, rebates, retainers, fixed monthly fees or opportunities for a mark-up? Describe in detail.
- Do we take steps to establish that compensation paid to third parties or derived by them in connection with our products/services is not excessive but is commensurate with market rates and the level of services provided? Explain.
- Do we have written agreements with all our third parties? Are there instances when written agreements are not necessary or can be waived? Do agreements with third parties have a defined term and expire if not expressly renewed? Are they automatically renewed?
- Do we ever use consultants or third parties with hard-to-define or hard-to-verify business justification and scope of work?
- Are our third parties whose contractual performance is not obvious required to provide periodic activity reports or other confirmation of their legitimate efforts on behalf of our company to justify the compensation? Does our organization review and validate these reports?
- Do we have contractual rights to audit our third parties periodically or when compliance issues arise? If so, how often do we audit our third parties? What is the process for selecting the audit targets?

Mergers & Acquisitions, Joint Ventures, Teaming Arrangements

- How often does our company engage in M&A transactions?
- How often do we enter into joint ventures, strategic partnerships, teaming arrangements or other cooperative relationships with other companies?
- Do we conduct compliance due diligence on acquisition targets, strategic partners, or potential joint venture or teaming arrangement partners before committing to the relationship? Explain.
- Are any of these transactions or relationships subject to government or regulatory approvals? How do we go about obtaining them? Do we use third parties for assistance?

Interaction with Government Officials

- Do we seek to recruit or hire former government or military officials or close relatives of government or military officials?
- Do we ever discuss employment opportunities with government officials or customers?
- Has our company employed, or offered employment to, current or former government officials or their relatives in the last 24 months?
    - Explain how these candidates were identified and the entire process of identifying, recruiting and hiring, along with determining their compensation, position, supervisors, etc.
    - What was the scope of their official government responsibilities before these former officials left government service?
    - Did we comply with any cooling-off or revolving door rules?
    - Did our company interact with them directly or indirectly while they were serving as government officials?
    - Were there any exceptions made to our normal recruitment and HR processes for such employees?
    - Are these employees subject to our normal HR processes (e.g. clear job description, compensation commensurate to the experience and value of work provided, normal annual performance reviews, self-evaluations, training, etc.)?
- Has our company paid for, offered help with, arranged or otherwise facilitated healthcare or education for current or former government officials or their relatives?
- Has our company received, considered or acted upon recommendations from government officials on which specific third parties to engage or hire? How often does this happen?
- Does our company or do our third parties offer gifts, hospitality or entertainment to government officials or customers? Explain.
- What policies, procedures and compliance measures do we have about gifts, hospitality and entertainment?
- Do we offer facility tours to customers or government officials or allow them to visit our facilities or other locations to demonstrate our capabilities and products/services? Explain (e.g. how often, who pays, any controls and compliance steps, approvals needed, etc.).
- Do we contract with or retain services of any companies associated with government or military officials or their family members? What safeguards do we take to identify and address any associated risks (e.g. vendor vetting, Politically Exposed Persons and reputational screening, due diligence)?

Financial Topics

- Do we have adequate financial controls and accounting processes that accurately reflect all company assets, resources and transactions?
- Do our accounting practices comply with applicable accounting standards (e.g. GAAP, IFRS)?
- Does our company have an effective internal audit function that is adequately staffed and has sufficient authority and resources?
- Are our financial statements periodically audited by reputable outside auditors?
- Have any serious weaknesses, financial control gaps or issues been identified in the last 24 months? Do they have any bearing on anti-bribery compliance matters? Explain. How have they been addressed or how are they being addressed?
- Does our company make payments in cash? If so, what is the process (e.g. approvals, where cash is kept, receipts, accounting)?
- Do we use petty cash? What is it used for? What is the process and what are the limits? How is the use accounted for?
- Are there off-books funds or expenditures or a second set of books? Is the answer the same for our subsidiaries in challenging jurisdictions that have an opaque legal environment, foreign currency controls, profit and capital repatriation restrictions, or other restrictions?
- Is off-budget/off-books spending allowed? Does it happen?
- Is any company spending mischaracterized or not accurately reflected on our books and records?
- Are there any ill-defined spending categories ("black boxes") that do not require detailed business justification, documentation and audit trail?
- Are there any atypical or disproportionately high spending categories that do not follow norms for similarly situated companies (e.g. third party commissions, office supply costs, housing allowances, transportation fees, freight forwarding costs, lobbying or charitable contributions, corporate social responsibility costs, etc.)?
- Think of the ways an employee or business unit could possibly embezzle corporate funds or accumulate off-books funds and conceal them from company management and books and records (e.g. generate false invoices, inflate or pad existing invoices, generate false reimbursement requests, use petty cash, make payments to sham consultants, request kickbacks from suppliers, inflate compensation or bonuses). What are some potential indications of such activity? Does our company adequately monitor for such red flags?
- If employees or third parties decide to make improper payments using their personal funds in the course of their work for our company, is there anything to stop them or to detect that this may have occurred? Are there incentives for them to engage in misconduct (e.g. large sales commissions)?

Human Resources and Employment Topics

- Do our compensation, incentive, bonus and promotion practices incentivize compliant behavior or excessive compliance risk-taking? Explain.
- How do we instill our corporate culture of compliance during the entire employment cycle from recruitment to employee onboarding to annual performance reviews, periodic training, certification and exit interviews?
- Do our performance evaluation and review processes address anti-corruption compliance requirements?
- What compliance complaints have we received over the last 24 months? How have they been handled? Are there any patterns or lessons learned?
- Does our company employ former government or military officials or their close relatives? What safeguards do we take to identify and address any associated risks?
- Is there a formal mechanism for employees to notify a designated company officer of suspected compliance violations or breaches of our company's code of conduct, policies and procedures?
- Are there clear disciplinary procedures for violating the code of conduct or policies and procedures? Are they communicated to the employees? Are instances of disciplining employees for misconduct made known to other employees?
- Do we have policies on protecting whistleblowers? How do they work in practice?

Controls and Compliance Measures

- Have leaders of our company established a checks and balances mechanism to prevent and detect unethical behavior and misconduct?
- Does our company management communicate a clear anti-corruption message to the entire company and ensure the implementation of policies, procedures and systems?
- Does our company have an effective code of conduct, policies, procedures and systems to prevent and detect unethical behavior and misconduct? Are they clear and easy to understand so that employees know what is expected of them?
- Does our company have anti-bribery policies and procedures and other relevant compliance policies (gifts, entertainment and hospitality; use of third parties; facilitation payments; conflicts of interest; whistleblower protections; monitoring and review; charitable donations and political contributions; patronage and sponsorships; lobbying and government relations)? Are employees able to explain the main requirements of those policies and procedures?

- Do we train our employees on these policies and procedures? How often? Is the training in person or through online modules? Are employees able to ask questions or raise concerns during or after the training? How does the company keep track of training progress?
- Do employees of our company adhere to the policies, procedures and systems in place?
- Do employees know about and know how to use our company's grievance redress channels (e.g. HR/legal/compliance department complaint processes, reporting hotline) to raise their concerns? Explain.
- Does our company have an anonymous or confidential hotline or other mechanism for alerting the company of concerns or suspected misconduct?
- Does our company have a dedicated robust compliance function that reports to the CEO and/or board of directors?
- Does the compliance function have sufficient authority and resources to address compliance issues that may typically arise?
- Describe the organization of the compliance function, the reporting lines, the staffing and resources available, and the mechanism.
- Are company authorities and responsibilities clearly defined and communicated to all parts of the business?
- How does our company manage third parties? How do we identify, recruit, vet and engage them?
- Do we conduct risk-based due diligence reviews and vetting of third parties before retaining them and periodically after that? How often?
- Do we have written agreements with all of our third parties? Do the agreements have a defined or indefinite term? Do the agreements renew automatically?
- Do agreements with third parties clearly describe the nature of the relationship, products to be delivered or legitimate services to be provided, and contain a clear detailed statement of work?
- Do we require third parties to contractually agree to anti-bribery compliance requirements?
- Do our agreements with third parties have termination rights? Explain.
- Do we monitor third parties for any compliance concerns after onboarding throughout the relationship?
- Do we perform an annual risk assessment to determine our company's exposure to bribery and corruption risks?
- Have there been any significant compliance issues or incidents in the last 24 months? Explain. How have they been addressed or how are they being addressed? Is there any pattern to these issues or incidents? Have they revealed any new or confirmed known corruption risks? Have we incorporated any lessons learned into our compliance program and internal controls?

- What compliance reports or complaints have we received in the last 24 months? Have they been adequately addressed? Are there any recurrent themes, patterns or lessons learned?

Risk Identification and Quantification

Many of the questions above may be supplemented with the following risk identification and quantification questions:

- What are possible government touchpoints and opportunities for corruption that may arise in this context?
- On a scale from 1 to 5 (see below), how likely is it that our company or our third parties may face bribe solicitations, be motivated to offer improper payments or risk engaging in other misconduct in connection with this issue/topic in the next 12 to 24 months?

5	> 90%	Almost certain
4	50-90%	Likely
3	20-50%	Possible
2	5-20%	Unlikely
1	< 5%	Rare

- On a scale from 1 to 5 (see below), how big of an impact or how disruptive would it be for our company if this risk materialized or our company failed in this respect?

5	Critical
4	Major
3	Moderate
2	Minor
1	Insignificant

Summary

- In your opinion, which of our company's business operations and processes are most likely to be affected by corruption?
- In summary, what are the top five corruption risks our company faces? What is their impact and likelihood of occurrence?
- What internal controls are most important in addressing these risks?

References

1 DOJ, SEC, A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition (2020) at 60.

2 U.K. Ministry of Justice, The Bribery Act 2010: Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (2011) ("UKMOJ Guidance") at 25. In its investigations and enforcement actions, the UK Serious Fraud Office follows the UKMOJ Guidance. See section "Evaluating a Compliance Programme" in the SFO Operational Handbook.

3 Article 7(II)(3) and (4) of Sapin II Law No. 2016-1691 (unofficially translated from French).

4 The French Anti-corruption Agency Guidelines to help Public and Private Sector Entities to Prevent and Detect Bribery, Influence Peddling, Extortion by Public Officials, Illegal Taking of Interest, Misappropriation of Public Funds and Favouritism (2021) ("AFA's Guidelines"; an English translation) at 18; AFA's Recommandations destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêts, de détournement de fonds publics et de favoritisme (2021) (in French).

5 DOJ's Evaluation of Corporate Compliance Programs at 3-4.

6 UKMOJ Guidance at 25-26.

7 AFA's Guidelines at 18-23.

8 DOJ's Evaluation of Corporate Compliance Programs at 3 and 12.

9 AFA's Guidelines at 20.

TRACE

TRACE is a non-profit international business association dedicated to anti-bribery, compliance and good governance. Founded in 2001 to make it easier and less expensive to navigate and mitigate business bribery risk, TRACE is credited with establishing anti-bribery standards that have been adopted worldwide. Driven by the needs of its members, TRACE is continuously developing tools and resources that power compliance programs. TRACE is headquartered in the United States and registered in Canada, with a presence on four continents.

For more information:

+1 410.990.0076

info@TRACEinternational.org

www.TRACEinternational.org

151 West Street, Annapolis, MD, USA 21401

Follow us on: