



# ADDRESSING CORRUPTION RISK

Through Enterprise Risk Management



## **ABOUT THE CENTER FOR RESPONSIBLE ENTERPRISE AND TRADE (CREATE.ORG)**

The Center for Responsible Enterprise And Trade (CREATE.org) is a non-governmental organization (NGO) helping companies around the globe prevent piracy, counterfeiting, trade secret theft, and corruption.

### **For More Information**

Please visit [www.CREATE.org](http://www.CREATE.org), via email at [info@create.org](mailto:info@create.org) or follow us on Twitter [@CREATE\\_org](https://twitter.com/CREATE_org).

# TABLE OF CONTENTS

---

## 02 OVERVIEW

## 04 THE BASICS OF ERM

- What is enterprise risk management?
- How does enterprise risk management work?

## 05 USING ERM TO MANAGE CORRUPTION-RELATED RISKS

- STEP 1: IDENTIFY: WHAT RISKS DOES THE COMPANY FACE?
- STEP 2: ASSESS: HOW SERIOUS ARE THOSE RISKS?
  - ° RESOURCE: SAMPLE ANTI-CORRUPTION RISK ASSESSMENT FORM
- STEP 3: MANAGE: WHAT STEPS SHOULD THE COMPANY TAKE TO MANAGE RISKS?

## 13 A MANAGEMENT-SYSTEM FRAMEWORK FOR MANAGING CORRUPTION RISKS

1. POLICIES, PROCEDURES AND RECORDS
2. COMPLIANCE TEAM
3. RISK ASSESSMENT
4. SUPPLY CHAIN MANAGEMENT
5. TRAINING AND CAPACITY BUILDING
6. MONITORING AND MEASURING
7. CORRECTIVE ACTIONS AND IMPROVEMENTS

## 14 CONCLUSION

## 15 APPENDIX A: COMPARISON OF RISK MANAGEMENT STANDARDS

## 17 ENDNOTES

---

# AN INTRODUCTION

In today's globalized marketplace, corruption poses significant risks that can impact a company's reputation, resources and its bottom line.

Ensuring that employees and partners are adhering to strong anti-corruption policies and practices can be a difficult task. Many companies do not go beyond the basics. Additionally, there is confusion about the different international guidelines, resource constraints, and when working with third parties, lack of visibility of compliance practices and push back on company efforts to require more.

Enforcement authorities in the U.S., UK and elsewhere have made it clear that they expect companies to put in place a risk-based and well-documented approach to anti-corruption compliance. As such, companies should take proactive, preventive measures that move beyond a 'contract-only' approach to embed anti-corruption practices into the business and communicate clear expectations and practices to employees and business partners alike.

This whitepaper describes how to use Enterprise Risk Management (ERM) to manage corruption-related risks. It examines how companies can use ERM more effectively to "identify, assess and manage" corruption risks and takes a close examination of effectively working with third parties.

Additionally, the whitepaper outlines the elements of an effective management system framework to prevent, detect and mitigate corruption risks.

The Center for Responsible Enterprise and Trade (CREATE.org) has produced this whitepaper to provide practical guidance for companies and their supply chain and business partners to improve and share leading practices for corruption prevention.

To learn more about CREATE, please visit [www.CREATE.org](http://www.CREATE.org) or email [info@CREATE.org](mailto:info@CREATE.org).

December, 2014



# OVERVIEW

Corruption poses significant strategic, operational, financial and reputational risks for any company doing business today. For companies with global operations, those risks can be daily realities. And as governments around the world are intensifying their focus on corruption through the adoption and enforcement of laws that target organizations and individuals, companies have all the more reason to mitigate these risks.

In the United States, enforcement of the Foreign Corrupt Practices Act (FCPA) continues at an aggressive pace;<sup>1</sup> but anti-corruption is no longer only within the purview of the U.S. The UK, Germany and Switzerland, too, are aggressively enforcing their anti-bribery laws,<sup>2</sup> and the landscape in China and Brazil is also improving, with a new focus on enforcement in China and a new, tough law in place in Brazil. In addition to governments, the multi-lateral development banks, which operate primarily in emerging markets, now routinely conduct anti-corruption investigations of bank-funded projects, with far-reaching consequences for companies, including debarment and referral of cases to country enforcement authorities.<sup>3</sup>

What is at stake for companies is more than the millions in criminal penalties that may be assessed for a violation and potential jail time for their executives. According to a 2014 report by the Center for Strategic and International Studies (CSIS), the face value of bribery, shareholder derivative suits, and other associated costs amounts to a \$515 billion “tax” on the private sector.<sup>4</sup>

External demand for compliance comes from other quarters as well. Investors, for example, are now demanding information about a company’s commitment to corruption prevention, and the European Union recently adopted a directive requiring companies to disclose information on their anti-corruption efforts, among other non-financial information.<sup>5</sup>

In this environment, it is essential for companies to ensure that they understand and can address corruption risk. Enterprise Risk Management (ERM)—the framework or set of processes


that companies use enterprise-wide to manage uncertainty and to determine how much risk to accept—is a useful tool for companies to do so.

Companies are increasingly implementing ERM as a corporate function to help assess the wide variety of risks they face, and then to implement plans to manage those risks. An effective risk management program will focus both on internal and external risk factors—particularly those posed among a company’s suppliers, distributors, sales agents and other business partners.

Companies can face any number of risks including financial stability, quality control, health and safety, environmental and labor issues. Similarly, corruption-related risks are sometimes also identified and managed using ERM. Many companies find that a common approach, implemented through the company’s management systems can help deal with a range of very different risks in an organized and integrated way. In this year’s Dow Jones Anti-Corruption Survey Results 2014, 27% of the 381 companies responding reported that they currently use an ERM system to assess bribery risk, down from 30% in 2013.<sup>6</sup>

More commonly, however, companies do not assess and manage risk in a holistic fashion. Nor do they necessarily address all of the risks they face in today’s global, interconnected and mobile economy. This includes corruption-related risks, which many companies do not assess in any detail. Others fail to consider how to manage corruption-related risks posed by third parties—a vital element for shifting from a reactive to a preventative approach.

Following the approach of the major ERM standards and frameworks, this paper examines how companies can use ERM more effectively to “identify, assess and manage” corruption-related risks, including insights into how to do so as the basis of a robust anti-corruption compliance program. It describes how management-system approaches that companies may already have in place for addressing other types of risks can be adapted to mitigate corruption risks as well.



“Companies use ERM to identify, assess and manage risks before they arise—and over time—in a compressive and intelligent way, rather than simply dealing with them ad hoc when they have gone from being a mere potential to an urgent problem.”

# THE BASICS OF ERM

**WHAT IS ENTERPRISE RISK MANAGEMENT?** Enterprise risk management is “a common framework applied by business management and other personnel to identify potential events that may affect the enterprise, manage the associated risks and opportunities and provide reasonable assurance that [company] objectives will be met.”<sup>7</sup> ERM has grown

Effective risk management should not increase bureaucracy at the expense of corporate flexibility and profitability. Quite the opposite—its overriding goal should be to protect and grow the value of a company. As the Committee of Sponsoring Organizations (COSO), an accounting industry consortium that has published an influential framework for developing and carrying out enterprise risk management, has noted,

*[E]very entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and*



substantially since the mid-1990s as a way for companies to identify, assess and manage various types of risks, with the goal of protecting and growing the company’s value. The insurance business and various financial markets have been engaged in certain kinds of risk management as far back as the 1950s. But attention to risk management has expanded and become more sophisticated with the appearance of more corporate-wide risks such as the “Y2K bug” in 1999, the increase in regulation, such as the Sarbanes-Oxley Act of 2002,<sup>8</sup> requiring companies to perform specific types of risk management in different areas, and the globalization of corporate sourcing and sales. This has led to the move by companies across business sectors toward more holistic management of corporate objectives and risks.

What was once viewed simply as contingency or insurance planning has developed more broadly into integrated programs of enterprise risk management involving an “ongoing process, in which objectives, risks, risk response measures, and controls are regularly re-evaluated.”<sup>9</sup>

*associated risk and opportunity, enhancing the capacity to build value.*<sup>10</sup>

## HOW DOES ENTERPRISE RISK MANAGEMENT WORK?

Companies use ERM to identify, assess and manage risks before they arise—and over time—in a comprehensive and intelligent way, rather than simply dealing with them ad hoc when they have gone from being a mere potential to an urgent problem. Seen in this light, ERM is a fundamental tool for helping companies shift from a reactive to a proactive, preventative approach to risk, and for strategically allocating resources to reduce risk internally and in the supply chain.

There are several frameworks that different industry and standards bodies have developed to structure the ERM process, but they all follow the basic approach that a company should **identify**, **assess** and then **manage** its risks. These steps are explained in more detail in the rest of this paper, with particular application to corruption-related risks.

# 1 IDENTIFY: WHAT RISKS DOES THE COMPANY FACE?

## USING ERM TO MANAGE CORRUPTION-RELATED RISKS

### Establishing the context

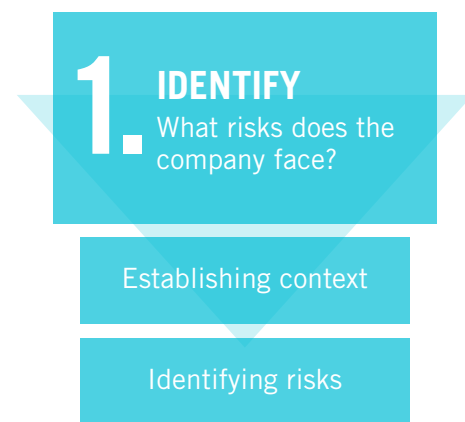
In order to promote holistic assessment of a company's risks, the major ERM frameworks and standards call for looking first at the relevant **context**—identifying the company's objectives, and its business, environment and other factors that affect the risks that it faces.<sup>11</sup>

When considering corruption risk, it is useful to understand the company's business objectives and its ethical and other values, as well as the following types of factors:

- the company's business objectives, and its ethical and other values,
- the legal, regulatory and business environment in which the company operates (**geographic** risk),
- the extent to which the company is heavily regulated, relies on government contracts or has a history of corruption-related incidents (**industry or sectoral** risk)
- business or organizational risks posed by the company's overall structure and its divisions, businesses, subsidiaries, and staff that are responsible for or otherwise deal with particular issues and risks, and the company's internal control structure,
- whether particular transactions involve unique risks such as charitable or political contributions; licenses or permits; public procurement projects; or include the use of intermediaries or agents (**transactional** risk).
- its relationship with and dependence on its business partners to carry out particular activities and functions (**third party** risks), and
- its risk management philosophy, and its risk tolerance.

## IDENTIFYING RISKS

Once this context is well understood, the next step in a typical ERM program is to generate a detailed list of the company's potential risks. In many companies, the process of identifying risks focuses on issues such as financial stability, quality control, health and safety, environmental and labor issues. However, as the risk of corruption increases, so should a company's focus on identifying it before a corruption event occurs.



As noted earlier, the best ERM programs include in their risk identification both their company's own internal risks and the risks that arise in the company's supply chain. This is a key point. The corruption risks companies face from their supply chain and business partners, including agents, distributors, vendors and others, have never been greater than they are in today's business environment. Rapid globalization has brought with it unprecedented opportunity for expansion and growth. But it has also multiplied certain risks, including the risks posed by actions taken by third parties. Corruption perpetrated by employees and business partners alike can take a heavy toll on a company's bottom line and reputation, and ensuring anti-corruption compliance by third parties who may be far removed from headquarters and over whom a company may have little control can be a complex task. With companies often relying on supply chains that cross multiple geographic boundaries to bring products and services to market, the challenge is how to balance these opportunities and risks.

Industry and standards groups divide corporate risks into different categories,<sup>12</sup> but these are summarized here as **strategic risks, operational risks, compliance risks, financial**



**risks** and **reputational risks**. These categories, of course, are flexible, and any particular risk may—and often does—fall into one or more of these areas.

- **Strategic risks** are those “big ticket items” that can affect a company’s overall mission, business objectives and strategy, market acceptance, future growth and/or shareholder value. These can arise externally or internally—from changes in the overall market situation or competitors’ activities to internal product and project difficulties and brand risks. For example, whether to enter a particular market or do business with a specific business partner can rise to the level of strategic risks.
- **Operational risks** involve problems and hazards that can arise in the day-to-day running of a company’s business and have a negative effect on the company’s income, profits and expenses. “These are the risks that are embedded in the assets of the organization, as well as the methods it uses to execute strategy—including people, process and technology.”<sup>13</sup> Corruption disrupts business operations by creating inefficiencies. When resources are diverted through bribery and corruption, business suffers. In addition, with the globalization of business, supply chain continuity and supply chain sustainability have become increasingly critical areas of operational risk, putting the compliance of third parties in the supply chain under more scrutiny. This is causing leading multinationals to push toward a more holistic risk assessment that includes identification of risks among such third parties.
- **Compliance risks** may be most associated with corruption. Compliance risks arise in areas covered by government regulation, industry standards or other undertakings. Failure to comply with anti-bribery, anti-fraud and other anti-corruption related laws and regulations are common compliance risks faced by companies and supply chains.
- **Financial risks** are the other major area where companies can face potential damage. These arise in such areas of financial statement reporting, (including violations of the FCPA and Sarbanes-Oxley),<sup>14</sup> financial controls, internal audits, credit problems, currency and interest rate fluctuation, and liquidity

and similar risks. Combined penalties, fines and disgorgement—in addition to the costs of investigation and remediation—from an anti-corruption enforcement action can total in the millions of dollars for companies. As an example, Wal-Mart has reportedly spent \$439 million in the past two years to investigate potential bribe payments in its global operations,<sup>15</sup> and with no clear end in sight, costs will no doubt continue to escalate. Siemens AG paid \$1.6 billion to resolve FCPA charges with the U.S. Department of Justice (DoJ), the Securities and Exchange Commission (SEC) and the Munich Public Prosecutor’s Office, and while this is still the largest sanction ever imposed in a bribery case,<sup>16</sup> total fines and penalties in bribery cases routinely total in the hundreds of millions of dollars. Companies and their Boards of Directors are also at risk for follow-on shareholder lawsuits. And once a company is known to pay bribes, it can become a target for future bribe solicitation.

- **Reputational risks** are broadly defined as exposure to the risk of events that undermine public trust in a company or its products or services. More formally, the U.S. Federal Reserve has issued the following definition: “Reputational risk is the potential that negative publicity regarding an institution’s business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.”<sup>17</sup> A company can suffer severe reputational damage—among customers, investors and business partners—from corrupt actions taken by its own employees and its supply chain and business partners.

## IDENTIFYING CORRUPTION-RELATED RISKS

Increasingly, both large and small companies alike recognize that corruption raises a variety of risks. The PricewaterhouseCoopers (PwC) 2013 State of Compliance survey of chief compliance officers found that corruption risk ranked among the top three risks faced by companies, and these risks were perceived to be increasing.<sup>18</sup>

## Public Companies Cite Corruption-related Risks in Securities Filings

Of the top 20 Fortune 500 companies, 40% specifically cited corruption-related risks as a “risk factor” that could seriously affect their business. Wal-Mart’s disclosure of corruption-related risks in its 2014 10-K illustrates the risks many multinational corporations face:

“In foreign countries in which we have operations, a risk exists that our associates, contractors or agents could, in contravention of our policies, engage in business practices prohibited by U.S. laws and regulations applicable to us, such as the Foreign Corrupt Practices Act and the laws and regulations of other countries such as the UK Bribery Act. We maintain policies prohibiting such business practices and have in place enhanced global anti-corruption compliance programs designed to ensure compliance with these laws and regulations. Nevertheless, we remain subject to the risk that one or more of our associates, contractors or agents, including those based in or from countries where practices that violate such U.S. laws and regulations or the laws and regulations of other countries may be customary, will engage in business practices that are prohibited by our policies, circumvent our compliance programs and, by doing so, violate such laws and regulations. Any such violations, even if prohibited by our internal policies, could adversely affect our business or financial performance.”

<http://www.sec.gov/Archives/edgar/data/104169/000010416914000019/wmt-form10-kx13114.htm>

corruption risk than other types of organizations. A company in the aerospace and defense or extractive industries working closely with and/or selling to governments will have a very different risk profile than one selling retail products directly to consumers.

Whatever an individual company’s case may be, it is important that it identify all of the possible types of strategic, operational, compliance, financial and reputation risks associated with corruption in its risk assessment and not simply the most obvious compliance risks, such as the potential negative consequences associated with an investigation or prosecution.

## 2. ASSESS: HOW SERIOUS ARE THOSE RISKS?

Once potential risks have been identified, the next step in enterprise risk management is to assess the risks. This includes an evaluation of both the probability or likelihood that a risk will actually be realized, and the relative severity or consequences that this would have on the company if it happened. Different standards and industry ERM frameworks divide this into different numbers of steps and sub-steps, and give these different names, but this is the heart of the “risk assessment” process.

### 2. ASSESS How serious are those risks?

Likelihood of occurrence

Consequences of occurrence

The risks any company will face, however, will vary by industry, market, and transaction, among other factors. Corruption is more common in certain markets and industries or lines of business. A company with a decentralized operating structure and loose financial controls will face more

## ASSESSING SPECIFIC CORRUPTION RISKS

There are a number of commonly-recognized risk areas that companies should consider when performing an anti-corruption risk assessment. Transparency International's Business Principles for Countering Bribery states that a company should consider "an enterprise's particular business circumstances and culture, taking into account such potential risk factors as size, business sector, nature of the business and locations of operations."<sup>20</sup>

The UK Ministry of Justice's The Bribery Act 2010 Guidance notes that "commonly encountered" bribery risk can fall into a number of categories, including country, sectoral, transactional, business opportunity and business partnership risks.<sup>21</sup>

Guidance issued by the DoJ and the SEC—FCPA, A Resource Guide to the U.S. Foreign Corrupt Practices Act—notes that risk factors to consider include "country and industry sector, the business opportunity, potential business partners, level of involvement with governments, amount of government regulation and oversight, and exposure to customs and immigration in conducting business affairs."<sup>22</sup>

For purposes of this paper, we have divided corruption risks into five categories: geographic, industry/sectoral, organizational, transactional, and third-party. Many of these categories overlap such that risks presented in one area may be relevant to those presented in another.

Technology can be an important tool for risk assessment, especially if your company does business in multiple markets or works with a large number of third parties. The categories below can be incorporated into a software program that aggregates and mines data to identify corruption risks.

### GEOGRAPHIC RISKS

A company should assess the risks for each market in which it operates. Information gathered from sources such as Transparency International can help a company evaluate the perceived risk of corruption in a given market. Locally-based resources, including company employees, local partners, embassies, and external consultants, such as investigators, lawyers, and accountants, may provide valuable insight as well. An assessment of geographic risk should include a review of anti-corruption laws, procurement regulations, enforcement activity, as well as the government's involvement

in the business sector either as a direct participant (i.e., through state-owned enterprises or government investment) or as a regulator (i.e., via required approvals, permitting or licensing, taxation or other regulatory oversight).

### INDUSTRY/SECTORAL RISKS

A company should assess the potential corruption risks specific to its industry, including whether it is subject to a high degree of regulatory scrutiny; the prevalence of government investigation and oversight; whether government agencies or state-owned enterprises make up a significant component of its customer base; and the historical pattern of corruption in its industry.

### ORGANIZATIONAL RISKS

It is also important to assess whether there are external factors specific to business operations that may make them more risky. These might include significant revenue from foreign governments; regular interaction with government officials, including customs, immigration, and border control; operations that depend on government contracts or critical licenses; and long-term operations such as joint ventures with government entities, including state-owned or state-controlled entities.

Organizational risks also encompass a company's external profile, such as whether it is one of the largest and/or most established in its sector; whether it is a new market entrant, whether it receives significant media coverage; and whether it has been involved in previous investigations or enforcement actions.

At this juncture, it is also crucial for a company to consider whether its internal operating structure may create risk. Factors to consider include whether it is centralized or decentralized; whether there are relevant organizational or cultural differences among various operations; and whether senior management sends a clear anti-corruption message.

Of particular importance is whether the anti-corruption processes or controls (i.e., the anti-corruption compliance program) the company already has in place are comprehensive and specifically tailored to the risks it has identified as part of the assessment process.

## TRANSACTIONAL RISKS

Next, consider the specific risks that may exist for a particular transaction. These will include evaluating the factors above, but also considering whether the particular transaction involves charitable or political contributions; requires inspection licenses or permits; involves a public procurement project; or includes the use of intermediaries or agents.

## THIRD-PARTY RISKS

Also consider the specific risks posed by different types of business partners. Again, these will include the factors above (e.g., geographic, industry/sectoral, organizational, transactional), but also include the identity of the third party, its ownership, track record and reputation; why the third party was selected (i.e., the ‘business justification’); how the third party will be compensated; and potential touch-points with government officials.

## LIKELIHOOD OF OCCURRENCE

Once a company has gone through the list of potential risks, determining how likely it is that any identified risk will occur is the next step in determining whether and how that risk should be addressed. This is not a strictly scientific process—predicting the future never is—but depending on the risk in question, its likelihood can often be determined at least in part based on objective elements such as the controls currently in place, previous incidents, equipment or system tolerances or failure rates, industry data, benchmarking, or probability models.

It is important to recognize that there will always be some uncertainty in estimating the likelihood of any particular risk happening. ERM systems thus tend to categorize the likelihood of risk in fairly broad categories, such as low, medium or high; or on a scale of one to four, or one to five; or in terms of a probability percentage.

## CONSEQUENCE OF OCCURRENCE

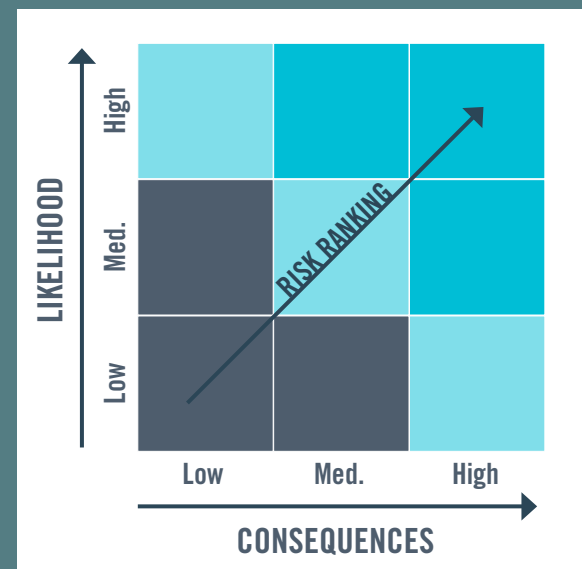
The other major element of risk assessment is estimating how serious the damage or negative impact on the business would be if any particular risk were actually realized. A company may be far more concerned about a low probability risk that could put the company out of business if it became a reality, than it might be in the case of a risk that is highly likely to occur but would have very little impact on the business.

As with predicting the likelihood of occurrence, estimating the consequence of a risk occurring is typically a mix of quantitative and qualitative, or objective and subjective,

factors. ERM assessments again use designations such as low, medium or high, or a scale of one to four or five, in categorizing the potential consequences of a risk.

It is important also to note that different risks may be related and thus have cumulative effects on the likelihood of other risks occurring, or knock-on implications for the consequences of other risks. It can be very helpful to identify where this may be the case—both as part of the risk assessment and in the next step of managing the company’s risks.

*Fig 2. Risk Likelihood and Consequences. Analyzing the likelihood and consequences of corruption and other corporate risks in a holistic way is vital for ranking risks and informing how risks should be managed.*



## PRACTICAL TOOL FOR EVALUATING LIKELIHOOD AND CONSEQUENCE OF RISKS

A sample risk-assessment matrix form follows. The risks listed previously in the ‘risk identification’ stage can be placed into this form and then ranked according to their likelihood and consequences, on a scale of low, medium and high. Again, this template is designed to be simple enough for smaller companies to use, but can be expanded to include more information and details as needed by larger enterprises.



# 3. MANAGE

## WHAT STEPS SHOULD THE COMPANY TAKE TO MANAGE RISKS?

### RISK MANAGEMENT GENERALLY

Having identified and assessed the company's potential risks, the next step in enterprise risk management is to develop a risk mitigation plan for managing those risks. The purpose of the risk mitigation plan is to systematically reduce risk by decreasing the likelihood of the negative event occurring and the negative impact if it does occur. A commonly used approach is for companies to seek to "Avoid, Minimize and/or Offset" the risks.

The steps involved in risk management involve not only deciding what **risk response** (if any) to take to address these risks (i.e. developing the risk mitigation plan), but also implementing those steps in the company's management systems; **communication** of relevant information to staff, and doing ongoing **monitoring and review** to ensure that those steps are carried out as planned and are evaluated and updated as needed over time.<sup>23</sup>

### RISK RESPONSE

Determining what response to take for each of the risks that the company has identified is not a purely mathematical function, as it involves weighing risks with differing likelihoods and impacts. At this stage, companies typically decide whether to "avoid, minimize or offset" each risk, and determine which of the range of possible risk responses they will take for each risk, such as:

- discontinuing particular activities to avoid the risk;
- implementing or enhancing various types of safeguards, including business processes that form a part of the company's anti-corruption compliance program;
- sharing the risk with others to minimize risk (e.g. through outsourcing particular activities); or
- seeking ways to offset the negative impact.

Ultimately, a company may decide to accept a certain risk as within its risk tolerance and take no action. Even if this is the case, the risk assessment is critical to allowing the company to make a conscious decision to accept the risk.

## 3. MANAGE

What steps should the company take to manage those risks?

Risk response

Communication

Monitoring and review

Some of the considerations that companies use in determining what action to take in response to a risk include:

- how effective a particular action might be in reducing either the likelihood of the risk, its potential impact or both;
- how much the action will cost in comparison to its benefits;
- whether the action or a group of actions will reduce more than one of the identified risks; and
- the company's tolerances for risk.

Using a well-designed ERM program, a company's response to individual risks will not be taken in isolation, but as a group and over the entire enterprise.

Ultimately, risk response should involve concrete implementation plans that include a number of control activities relevant to the particular risks—ranging, for example, from any number of different corporate policies and procedures, to financial, accounting, recordkeeping and information technology controls, to employee and third party training, to monitoring compliance.<sup>24</sup> A company's responses to risk may be fairly straightforward, particularly for small and medium companies, or may require input, study and implementation planning.

Indeed, incident response plans are increasingly being developed by companies as tools to be used in many risk areas in case a negative event does occur. Typically the incident response plan covers what the company should do during the event, how it will minimize the ongoing damage from the event, and how it should change its controls or "management systems" to reduce the severity and probability of it happening again.

### COMMUNICATION

Communication, both internally with employees and externally with suppliers, distributors, business partners and other relevant stakeholders, is another vital component

of ERM, and is a two-way street. In identifying and assessing risks and responses to those risks, a company needs good data from all relevant departments, groups and personnel. Similarly, in responding to risks, good communication with all relevant departments, groups and personnel is essential for the company to convey what needs to be done, by whom, and how.

## MONITORING AND REVIEW

Effective risk assessment and risk management is not a one-shot exercise, but rather an ongoing program that needs to be reviewed, adapted, measured and improved over time. Risk factors themselves change, as do the potential likelihood and severity of these risks for the company. Monitoring and review are critical elements of managing risks through a continual improvement cycle, which is at the heart of the management-systems approach.

Following risk identification, risk assessment, and the development of risk-response plans, there are important questions to be answered, such as how particular risk responses have actually been implemented, whether the responses have been effective, and how they might be improved to manage the company's risks more effectively going forward. Selecting what to monitor is an important consideration. Effective monitoring looks at a combination of performance and process indicators. All of these considerations can and should be dealt with on an ongoing basis, through regular monitoring and periodic reviews—well-recognized elements of any good management system that are particularly important for a company's risk management program.

## MANAGING CORRUPTION RISKS IN AN INTEGRATED WAY THROUGH THE COMPANY'S MANAGEMENT SYSTEMS

A comprehensive risk assessment will help direct the efficient use of company resources, and ultimately, will serve as the base upon which an effective anti-corruption compliance program or "management system" is established, maintained and continually improved. The challenge in taking steps to manage corruption and other corporate risks is how to do so in a practical and sustainable way, embedding risk management in a company's overall business operations without undue costs or management resources, and without overlapping systems or repetitive activities.

Fortunately, it is not necessary to "reinvent the wheel" to manage corruption-related risks in most companies.

Companies can leverage existing management systems or controls already in place to manage other types of risks to address corruption-related risks internally and among its supply chain and business partners as well. Linking corruption controls to an overall enterprise risk management program not only helps to ensure that all of the company's potentially significant business risks get adequate consideration, it also helps to avoid duplication of management time and attention and takes advantage of existing processes and management systems to address corruption risks alongside many others in an integrated way.

Implementing risk responses (including control activities) that address multiple risks can substantially improve the cost-benefit calculation for implementing needed improvements. It makes much more sense to implement controls that address several related risks at the same time, for both internal and supply chain risks (e.g. internal company policies that business partners are also expected to implement and comply with), and multiple objectives (e.g. supply-chain risk assessments that evaluate not just anti-bribery but also intellectual property, environmental, labor and other compliance risks).

Of course, effective risk management requires collaboration and cross-functional support inside a company to address the range of related risks faced in an integrated way. It requires sending a clear and consistent message to employees and business partners on risk-related issues. A company's senior leadership has to make a clear commitment to the overall effort and communicate this to employees and business partners. It may even be necessary or advisable for a company to collaborate with other companies in its sector or geography to help raise the overall level, scope and consistency of risk assessment and risk management on such issues.

In a well-integrated enterprise risk management program, a company can make informed decisions about how appropriately to use its existing resources to strengthen its ability to mitigate potential threats. With the potential likelihood and impact of particular corruption risks having been analyzed alongside other corporate risks, and with a management-systems approach that seeks to manage a company's overall risks in a holistic way, a company can determine the best, most cost-effective means of reducing or otherwise mitigating these risks.



# A MANAGEMENT-SYSTEM FRAMEWORK FOR MANAGING CORRUPTION RISKS

CREATe.org has developed a management-system framework based on internationally-accepted leading practices that can help a company identify various areas within its own and its third parties' operations where corruption-related risk management is necessary. The framework comprises leading practices in seven key areas that a company can use to implement risk responses and controls to respond to corruption risk within its own and its supply-chain and business partners' operations:

## 1. POLICIES, PROCEDURES AND RECORDS

As in other areas of corporate operations and compliance, **company policies and procedures** establish the rules and mechanisms for preventing, detecting and remediating corruption, and they should respond to the actual risks that a company faces. A company's financial **books and records** must be accurate and complete, and it should develop and maintain **records** that document each aspect of its anti-corruption compliance program to sufficiently demonstrate the effectiveness of the program should that become necessary. As part of its risk assessment, a company should determine whether currently-existing policies and procedures are adequate to address identified risks

and whether they provide clear guidance to employees and others. Where they are not, it should enhance them as part of its risk response.

## 2. COMPLIANCE TEAM

Anti-corruption compliance needs a specified **company executive "owner,"** and is best managed by a **cross-functional team** representing relevant areas such as legal, compliance/risk management, finance, and audit, among others. This team may be corruption-specific or may be one that deals with multiple areas of risks for the company. Responding to corruption-related risks may require the establishment of such a team, or the addition of corruption risks to an existing team's mandate.

## 3. RISK ASSESSMENT

Some companies simply do not identify, assess and manage their corruption-related risks in any integrated way, but instead only take action reactively in response to particular problems that arise. Doing ongoing **corruption-related risk assessments** as part of a company's overall ERM program, is vital to strategically allocating



resources, ensuring a company’s anti-corruption compliance program is effective, and ultimately helping to reduce corruption-related risks internally and in its supply chain.

## 4. SUPPLY CHAIN MANAGEMENT

As discussed at length, corruption risks of all sorts can and do arise not only internally within a company but also among its supply chain and business partners. Systems for effective due diligence of business partners’ **policies and procedures** that partners are expected to implement and follow, and other ongoing **supply chain reporting and management requirements** should be in place to manage corruption risks. Similarly, the **contracts** that a company enters into with its supply chain and business partners should clearly spell out compliance requirements (including an agreement to cooperate with corruption-related investigations or other inquiries) and include audit rights. Part of the risk assessment is to ensure these processes are adequate to the task, and if not, to strengthen them. Again, it is typically not necessary to develop entirely new programs to implement such corruption risk-treatment steps with business partners; these can be integrated into the ongoing supply chain management that the company already uses to deal with other similar types of risks and issues.

## 5. TRAINING AND CAPACITY BUILDING

Even if a company’s anti-corruption program and corruption risk management systems are first rate, ongoing, risk-based **compliance training for relevant employees and supply chain or business partners**, and specialized training for employees exposed to higher risk, are necessary to ensure that all stakeholders understand anti-corruption compliance requirements and have the know-how to follow them. Anti-corruption policies and procedures are unlikely to be effective unless companies communicate clearly what they are and how to adhere to them. Ongoing training for relevant employees and third parties is a necessary part of anti-corruption risk management.

## 6. MONITORING AND MEASURING

Enterprise risk management is not a “one shot” exercise, but is an ongoing program that needs to be **monitored** and **measured** over time to be sure that it is producing the desired results. Implementing such an ongoing process will be needed if it is not already part of the risk management team’s mandate. Similarly, anti-corruption

compliance programs must also be **monitored** and **measured** over time to ensure effectiveness. Risk assessments should help determine if monitoring protocols are sufficient and if they address the highest risks faced by a company.

## 7. CORRECTIVE ACTIONS AND IMPROVEMENTS

**Dealing with specific corruption-related problems** through timely investigation and effective discipline is of paramount importance of course, but it is important that issues are not viewed simply in isolation or dealt with ad hoc. Performing a root-cause analysis of problems that arise, and making systematic updates and improvements to the company’s anti-corruption program and risk management approach, are vital to reducing corruption-related risks over time.

### EFFECTIVE ANTI-CORRUPTION COVERS 7 CATEGORIES

1. POLICIES, PROCEDURES & RECORDS	2. ANTI-CORRUPTION COMPLIANCE TEAM
3. SCOPE & QUALITY OF RISK ASSESSMENT	4. MANAGEMENT OF SUPPLY CHAIN
5. TRAINING & CAPACITY BUILDING	6. MONITORING & MEASUREMENT
7. CORRECTIVE ACTIONS & IMPROVEMENTS	

## CONCLUSION

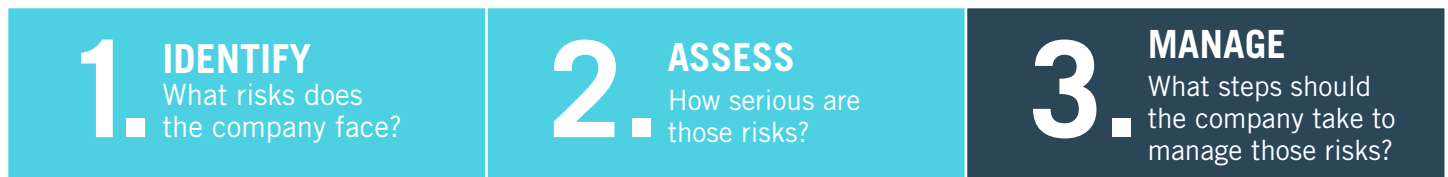
Enterprise risk management can be an effective tool to identify and measure the relevant corruption-related risks that can arise within a company and its supply chain; and ERM can provide a framework to implement risk-management steps as described in this paper to avoid, minimize or offset those risks to an acceptable degree. If corruption-related risks are considered alongside the other strategic, operational, compliance, financial and reputational risks that a company faces, these can all be assessed and managed in integrated ways that are both cost effective and of potentially great value to the company.

# APPENDIX A

## COMPARISON OF RISK MANAGEMENT STANDARDS

Different ERM standards and frameworks divide up the basic steps of identifying/assessing/managing risks in different ways. ISO's 31000 series Enterprise Risk Management standards identify the elements of ERM as Establishing Context, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, and Communication and Consultation.<sup>25</sup> The COSO framework divides these into somewhat more detailed steps, specifying the elements of an ERM program to include Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information and Communication, and Monitoring.<sup>26</sup> The Institute of Risk Management's 2002 standard calls for establishing Strategic Objectives, doing Risk Analysis, Risk Evaluation, Risk Reporting and Risk Decision, then doing Risk Treatment, Residual Risk Reporting and Monitoring.<sup>27</sup> These are compared below.

Obviously if a company intends to be formally certified to one or more of these standards, it will need to organize its ERM and document its activities using the categories of the particular standard chosen. A more flexible approach to structuring a company's ERM process, but one that still takes into consideration the same types of elements examined under the formal standards, may be appropriate for small and medium companies and others that want to improve their corruption-related risk management but do not necessarily seek formal standards certification.



### ISO 31000 RISK ASSESSMENT GUIDELINE:

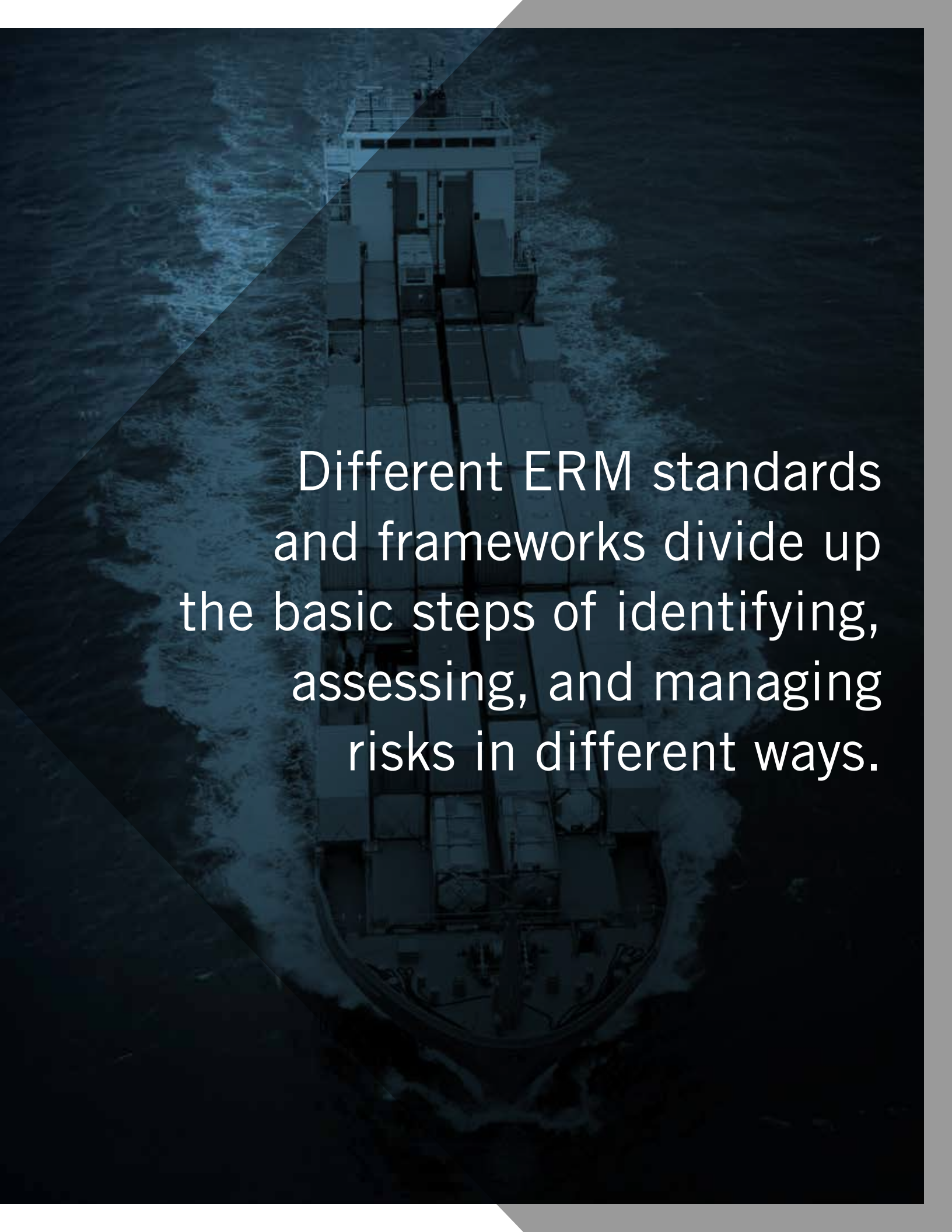
Context	Risk Identification	Risk Analysis	Risk Evaluation	Risk Treatment	Communication & Consultation
---------	---------------------	---------------	-----------------	----------------	------------------------------

### COSO FRAMEWORK:

Internal Environment	Objective Setting	Event Identification	Risk Assessment	Risk Response	Control Activities	Information & Comm.	Monitoring
----------------------	-------------------	----------------------	-----------------	---------------	--------------------	---------------------	------------

### IRM RISK MANAGEMENT STANDARD 2002:

Strategic Objectives	Risk Analysis	Event Evaluation	Risk Reporting	Decision	Risk Treatment	Residual Risk Reporting	Monitoring
----------------------	---------------	------------------	----------------	----------	----------------	-------------------------	------------

An aerial photograph of a large cargo ship sailing on the ocean. The ship is viewed from above, showing its deck with several rows of stacked cargo containers. The ship's wake is visible in the water. The image is dark and has a blue tint. A large, semi-transparent white triangle is overlaid on the left side of the image, pointing towards the center. The text is centered within this triangle.

Different ERM standards and frameworks divide up the basic steps of identifying, assessing, and managing risks in different ways.

# ENDNOTES

<sup>1</sup> SHEARMAN & STERLING LLP, FCPA DIGEST, at iv-v (Jan. 2014), available at <http://shearman.symplicity.com/files/4d5/4d5544d54cc00e81159f270a9d31dcb2.pdf>.

<sup>2</sup> FRITZ HEIMANN ET AL., TRANSPARENCY INTERNATIONAL, EXPORTING CORRUPTION – PROGRESS REPORT 2014: ASSESSING ENFORCEMENT OF THE OECD CONVENTION ON COMBATING FOREIGN BRIBERY 6 (Oct. 2014), available at [http://files.transparency.org/content/download/1573/11296/file/2014\\_ExportingCorruption\\_OECDProgressReport\\_EN.pdf](http://files.transparency.org/content/download/1573/11296/file/2014_ExportingCorruption_OECDProgressReport_EN.pdf).

<sup>3</sup> Glenn Ware & Arjun Ponnambalam, An Emerging Multi-Polar Enforcement Landscape, ABA CRIM. JUST. SEC. NEWSL., Winter 2014.

<sup>4</sup> DANIEL F. RUNDE ET AL., THE COSTS OF CORRUPTION: STRATEGIES FOR ENDING A TAX ON PRIVATE-SECTOR-LED GROWTH, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES 31 (Feb. 2014), available at [http://csis.org/files/publication/140204\\_Hameed\\_CostsOfCorruption\\_Web.pdf](http://csis.org/files/publication/140204_Hameed_CostsOfCorruption_Web.pdf).

<sup>5</sup> GEORGE DALLAS, BUSINESS ETHICS IN EMERGING MARKETS AND INVESTOR'S EXPECTATION STANDARDS, INTERNATIONAL CORPORATE GOVERNANCE NETWORK'S 2012 YEARBOOK (2012), available at <http://blogs.law.harvard.edu/corpgov/2013/01/19/business-ethics-in-emerging-markets-and-investors-expectations-standards/>; Press Release, Council of the European Union, New Transparency Rules on Social Responsibility for Big Companies (Sep. 29, 2014), available at [http://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/intm/144945.pdf](http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/intm/144945.pdf).

<sup>6</sup> DOW JONES, ANTI-CORRUPTION SURVEY RESULTS 2014, at 10 (2014), available at <http://images.dowjones.com/company/wp-content/uploads/sites/15/2014/04/Anti-Corruption-Survey-Results-2014.pdf>.

<sup>7</sup> JOHNSON & JOHNSON, FRAMEWORK FOR ENTERPRISE RISK MANAGEMENT (2013), available at [http://www.jnj.com/sites/default/files/pdf/JnJ\\_RiskMgmt\\_ERMFramework\\_guide\\_v16a.pdf](http://www.jnj.com/sites/default/files/pdf/JnJ_RiskMgmt_ERMFramework_guide_v16a.pdf).

<sup>8</sup> Sarbanes-Oxley Act of 2002, 15 U.S.C. §§ 7201-66 (2014).

<sup>9</sup> PRICEWATERHOUSECOOPERS (“PWC”), A PRACTICAL GUIDE TO RISK ASSESSMENT 6 (Dec. 2008) [“PWC GUIDE”], [http://www.pwc.com/us/en/issues/enterprise-risk-management/assets/risk\\_assessment\\_guide-rdt.html](http://www.pwc.com/us/en/issues/enterprise-risk-management/assets/risk_assessment_guide-rdt.html); see generally G. Dickinson, Enterprise Risk Management: Its Origins and Conceptual Foundation, 26 GENEVA PAPERS ON RISK & INS. 360, 360-61 (2001), <http://www.actuaries.org.uk/sites/all/files/documents/pdf/dickinson-g-2001-enterprise-risk-management-its-origins-and-conceptual-foundation-3.pdf>.

<sup>10</sup> COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), ENTERPRISE RISK MANAGEMENT — INTEGRATED FRAMEWORK: EXECUTIVE SUMMARY 1 (Sept. 2004) [hereinafter “COSO FRAMEWORK”], available at [http://www.coso.org/documents/COSO\\_ERM\\_ExecutiveSummary.pdf](http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf).

<sup>11</sup> The COSO Framework calls for Internal Environment

and Objective Setting to be evaluated before any risk Event Identification takes place. Id. at 3-4. The International Standards Organization (ISO) 31000 risk management standards series includes Establishing the Context as a step distinct from actually identifying and assessing risks. INTERNATIONAL STANDARDS ORGANIZATION (ISO) 31000, RISK MANAGEMENT – PRINCIPLES AND GUIDELINES 15-17 (2009) [hereinafter ISO GUIDELINES], available at [http://www.iso.org/iso/catalogue\\_detail?csnumber=43170](http://www.iso.org/iso/catalogue_detail?csnumber=43170). The Institute for Risk Management (IRM) 2002 standard calls for understanding the company's Strategic Objectives. THE INSTITUTE FOR RISK MANAGEMENT (“IRM”), A RISK MANAGEMENT STANDARD 4-5 (2002), available at [http://www.theirm.org/media/886059/ARMS\\_2002\\_IRM.pdf](http://www.theirm.org/media/886059/ARMS_2002_IRM.pdf). See also CREATE.ORG, PROTECTING INTELLECTUAL PROPERTY THROUGH ENTERPRISE RISK MANAGEMENT (2014) [hereinafter IRM STANDARD], available at <https://create.org/resource/protecting-intellectual-property-enterprise-risk-management/>.

<sup>12</sup> COSO categorizes risks as strategic, operations, reporting or compliance risks. See COSO FRAMEWORK, supra note 3, at 3. PriceWaterhouseCoopers lists the types of risks frequently assessed as strategic, operational, compliance, internal audit, financial statement, fraud, market, credit, customer, supply chain, product, security, information technology, and project risks. PWC GUIDE, supra note 2, at 9-11. The Institute for Risk Management categorizes risks as hazard or pure risks, control or uncertainty risks, and opportunity or speculative risks. P. HOPKIN, FUNDAMENTALS OF RISK MANAGEMENT 15 (2d ed. 2012).

<sup>13</sup> Leveraging 10 Years of SOX for Stronger Risk Management, RISK & COMPLIANCE J., Dec. 17, 2013, <http://deloitte.wsj.com/riskandcompliance/2013/12/17/leveraging-10-years-of-sox-for-stronger-risk-management/>.

<sup>14</sup> Foreign Corrupt Practices Act of 1977, 15 U.S.C. §§ 78dd-1-78dd-3, 78m, 78ff (2014); Sarbanes-Oxley Act of 2002, 15 U.S.C. §§ 7201-66 (2014).

<sup>15</sup> David Voreacos & Renee Dudley, Wal-Mart Says Bribe Probe Cost \$439 Million in Two Years, BLOOMBERG, March 26, 2014, available at <http://www.bloomberg.com/news/2014-03-26/wal-mart-says-bribery-probe-cost-439-million-in-past-two-years.html>.

<sup>16</sup> Press Release, Department of Justice, Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to Pay \$450 Million in Combined Criminal Fines (Dec. 15, 2008), available at <http://www.justice.gov/archive/opa/pr/2008/December/08-crm-1105.html>.

<sup>17</sup> FEDERAL RESERVE BOARD, EXAMINATION STRATEGY AND RISK-FOCUSED EXAMINATIONS, COMMERCIAL BANK EXAMINATION MANUAL, at 4.5 (April 2011), available at <http://www.federalreserve.gov/boarddocs/SupManual/cbem/1000.pdf>.

<sup>18</sup> PWC, DEEPER INSIGHT FOR GREATER STRATEGIC VALUE: STATE OF COMPLIANCE 2013 SURVEY 8 (2013) available at, [http://www.pwc.com/en\\_US/us/risk-management/assets/pwc-soc-survey-2013-final.pdf](http://www.pwc.com/en_US/us/risk-management/assets/pwc-soc-survey-2013-final.pdf).

<sup>19</sup> The ISO standard has three separate steps for Risk Analysis, comprising Controls Assessment, Consequence Analysis, and Likelihood Analysis and Probability Estimation. INTERNATIONAL ELECTROTECHNICAL COMMISSION (“IEC”) & ISO, IEC/ISO 31010:2009: RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES 9-10 (2009). The COSO framework simply terms these steps Likelihood and Impact, COSO Framework, supra note 11, at 4. The IRM standard labels these “Probability” and “Consequences”. IRM STANDARD, supra note 12, at 6-8. Many organizations classify risk by “Probability of Occurrence” and “Severity of Negative Impact.” Regardless of the specific terms used, the concept is the same.

<sup>20</sup> TRANSPARENCY INTERNATIONAL, BUSINESS PRINCIPLES FOR COUNTERING BRIBERY (2013), available at [http://www.transparency.org/whatwedo/tools/business\\_principles\\_for\\_countering\\_bribery](http://www.transparency.org/whatwedo/tools/business_principles_for_countering_bribery).

<sup>21</sup> MINISTRY OF JUSTICE, THE BRIBERY ACT 2010: GUIDANCE ABOUT PROCEDURES WHICH RELEVANT COMMERCIAL ORGANIZATIONS CAN PUT INTO PLACE TO PREVENT PERSONS ASSOCIATED WITH THEM FROM BRIBING (2010), available at <http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf>.

<sup>22</sup> SECURITIES EXCHANGE COMMISSION & DEPARTMENT OF JUSTICE, A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT (2012), available at <http://www.justice.gov/criminal/fraud/fcpa/guide.pdf>. For a comprehensive view of internationally-recognized guidance in this area see the CREATE Anti-Corruption Guideline Reference, available at <https://create.org/resource/anti-corruption-compliance-guidelines-english/>.

<sup>23</sup> The ISO standard calls these steps Risk Treatment, Communication and Consultation, and Monitoring and Review. ISO GUIDELINES, supra note 12, at 9-11. COSO divides these steps into the somewhat more detailed categories of Risk Response, Control Activities, Information and Communication, and Monitoring. COSO FRAMEWORK, supra note 11, at 4.

<sup>24</sup> Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity’s objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. COSO, INTERNAL CONTROL - INTEGRATED FRAMEWORK 2 (1992), available at <http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf>.

<sup>25</sup> ISO GUIDELINES, supra note 12; see generally D. Gjerdrum & M. Peter, The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework, SOC’Y OF ACTUARIES (Mar. 2011), <https://www.soa.org/library/newsletters/risk-management-newsletter/2011/march/jrm-2011-iss21-gjerdrum.aspx>.

<sup>26</sup> COSO Framework, supra note 11, at 3-4.

<sup>27</sup> IRM Standard, supra note 12, at 4.