IPPF

International Professional Practices Framework

Supplemental Guidance
Practice Guide

Auditing Anti-corruption Activities

2nd Edition

The Institute of Internal Auditors | *Global*

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.

Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- International Standards for the Professional Practice of Internal Auditing.
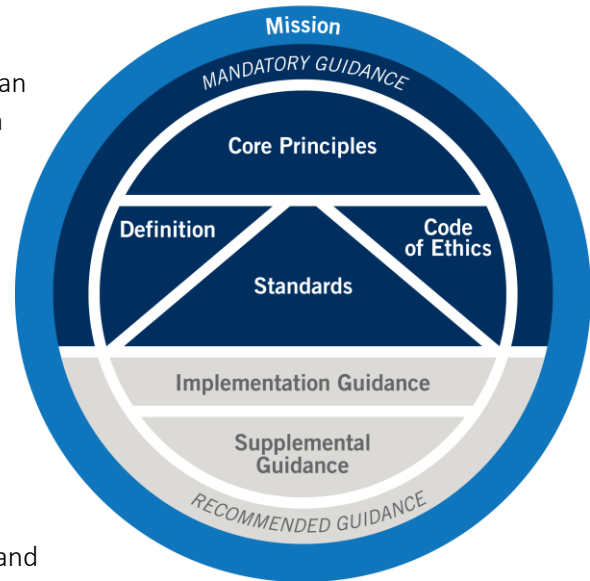
Recommended Guidance includes Implementation and Supplemental Guidance. Implementation Guidance is designed to help internal auditors understand how to apply and conform with the requirements of Mandatory Guidance.

About Supplemental Guidance

Supplemental Guidance provides additional information, advice, and best practices for providing internal audit services. It supports the *Standards* by addressing topical areas and sector-specific issues in more detail than Implementation Guidance and is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides, a type of Supplemental Guidance, provide detailed approaches, step-by-step processes, and examples intended to support all internal auditors. Select Practice Guides focus on:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

Table of Contents

Executive Summary

Regardless of the geographic location, industry, or type of organization or program, opportunities for corruption present significant risks. According to Transparency International's 2020 Corruption Perceptions Index, 17 of the world's 20 most populous countries scored 50 or below (out of 100) on perceived levels of public sector corruption, as rated by experts and business people, indicating that a majority of the globe's residents live in areas in which corruption is prevalent. Indeed two-thirds of the report's 180 countries and territories scored 50 or below, with an average score of 43.[1] Worldwide, corruption puts businesses and governments at risk and affects organizations, private individuals, and public officials.

This practice guide discusses the role of an organization's internal audit activity in anti-corruption efforts and describes an effective anti-corruption program, including controls related to preventing, detecting, responding to, and recovering from the risks associated with corruption.

The guide also provides an approach to assessing the maturity of an organization in terms of how management assesses and implements measures to mitigate the risks of corruption, and provides a closer look at the internal audit activities and procedures that may be performed as a function of that level of maturity.

Introduction

The definition of "**corruption**" has changed over time, but could be generally described as the use of power, money, or favors by people in positions of authority or contacts in their network for illegitimate private gain.

Note: Terms in bold are defined in the glossary in Appendix B.

The Organisation for Economic Co-operation and Development (OECD) has championed the global anti-corruption movement for about five decades. According to its website, "The overarching objectives of the organization's anti-corruption and integrity (ACI) work is to support trustworthy institutions and open, efficient, and inclusive markets. These objectives are aligned with the OECD's commitment to promoting policies that will improve the economic and social well-being of people around the world."[2]

Activities that influence the markets, undermine the public trust, or oppress people are forms of corruption. Forms of corruption vary widely but may include:

---

1. Transparency International, "Corruption Perceptions Index 2020," https://www.transparency.org/en/cpi/2020/index/nzl.

2. Organisation for Economic Co-operation and Development. n.d. "OECD Work on Anti-corruption and Integrity." Accessed July 12, 2021. https://www.oecd.org/corruption-integrity/about/.

- *Bribery*: Money or favor given or promised to influence the judgment or conduct of a person in a position of trust.

- *Extortion*: Demands for money or other payment in return for "protection" from (real or hypothetical) threats from unspecified other parties (this is related to racketeering, which occurs at the state and federal levels).

- *Nepotism/cronyism*: The appointment of family (nepotism) or friends (cronyism) to positions of authority without proper regard to their qualifications.

- *Influence peddling*: The use of position or political influence on someone's behalf in exchange for money or favors.

- *Bid rigging*: A fraudulent scheme in procurement auctions resulting in noncompetitive bids; can be performed by corrupt officials, by firms in an orchestrated act of collusion, or between officials and firms.

- *Misuse of funds*: Theft or misappropriation of funds placed in one's trust or belonging to one's employer (e.g., embezzlement).

Misuse of power for other purposes, such as repression of opponents or competitors; and general brutality toward others whether they be customers, employees, or the general public; are also considered corruption.

Additional Resource

See the Internal Audit Foundation's publication "Auditing Anti-Bribery Programs" for information supporting internal audit's proactive role in an organization's anti-bribery initiatives.

Risk Environment

Corruption puts governments, businesses, and people worldwide at **risk** and affects organizations, private individuals, and officials. Criminal activity can occur wherever money changes hands or other material gain is to be had. Corruption exposes organizations to risks in achieving operations, reporting, and **compliance** objectives, and may result in:

- Stifled market competition.
- The impediment of economic growth.
- Corroding of the global economy.
- Barriers to improved standards of living.
- Compromised product quality.
- Higher prices.
- Diminished trust.
- Discouragement of foreign direct investment.

Increasing globalization, legal complexities, and potential for serious financial and reputational harm have increased the risk exposure incurred by doing business with corrupt organizations or people. Organizations should establish anti-corruption activities including policies, controls, training, and anti-corruption compliance and other monitoring mechanisms to mitigate this risk. The implementation of these activities may require a team of subject matter experts with collective expertise in law, compliance, fraud, investigations, regulatory affairs, IT, finance, culture, and ethics. Internal audit may provide advice or consulting services on auditing the implementation of activities.

Case Study

"In the Maldives, tourism is the largest contributor to the economy – it's where the money is.

"A 2018 scandal saw the Maldives government lease more than 50 islands and submerged coral lagoons to tourism developers in no-bid deals.

"At least US$79 million from the lease fees was embezzled into private bank accounts and used to bribe politicians.

"The scandal implicated local businessmen and international tourism operators as well as former president Abdulla Yameen, who allegedly received US$1 million in funds."

Source: 25 Corruption Scandals that Shook the World, July 5, 2019, https://www.transparency.org/en/news/25-corruption-scandals.

Regulatory Landscape

Many countries have enacted legislation to curb corruption. Anti-corruption laws can fundamentally affect how individuals work, and many have international implications.

One of the strictest legal regulations designed to combat corruption is the United Kingdom's Bribery Act of 2010 (UK Bribery Act), which states: "An offence is committed under section 7 [Failure of commercial organizations to prevent bribery] irrespective of whether the acts or omissions which form part of the offence take place in the United Kingdom or elsewhere."[3]

Regulations such as this allow the prosecution of corruption charges in the UK no matter where the offense occurred. For example, according to the quoted provision, a UK company domiciled in London, England, can be prosecuted for violations of the UK Bribery Act occurring in a subsidiary located in Malaysia, regardless of whether the action is in violation of Malaysian law.

Global anti-corruption and anti-bribery resources are provided in Appendix G.

Bribery as a Business Model

"Ten years ago a colossal corruption scandal involving Siemens, one of the world's largest electrical engineering companies, shocked the world. The scale of it marked it out as the biggest corruption case of the time.

"A few years later, Linda Thomsen, director at the Security Exchange Commission [*sic*], described the pattern of bribery in the company as: '…unprecedented in scale and geographic reach. The corruption involved more than $1.4 billion in bribes to government officials in Asia, Africa, Europe, the Middle East and the Americas.'"

Source: Bertrand Venard, "Lessons from the massive Siemens corruption scandal one decade later," *The Conversation*, Dec. 13, 2018. https://theconversation.com/lessons-from-the-massive-siemens-corruption-scandal-one-decade-later-108694.

Anti-corruption Activities

Guided in part by anti-corruption legislation, some organizations with international operations have developed formal anti-corruption programs, while other organizations have implemented less formal but not necessarily less effective anti-corruption activities. Although approaches vary by organization, the elements in Figure 1 are essential to effective anti-corruption efforts.

---

3. UK Bribery Act, 2010, c. 23, last modified January 12, 2020. https://www.legislation.gov.uk/ukpga/2010/23/enacted.

Figure 1. Elements Needed to Fight Corruption in Organizations

Source: The IIA

Tone at the Top

Effective risk mitigation starts with a strong tone at the top, which sets the foundation for an organization's overall compliance framework. The tone at the top drives the culture of the organization and is perhaps the single most important factor in determining the organization's resistance to corruption. No system of controls can provide absolute assurance against the commission of corrupt acts; however, the **board** should insist on a tone at the top that promotes and rewards honest action by employees.

Additional Resources

IIA practice guides "Auditing Culture" and "Auditing Conduct Risk" provide detailed information on how an organization's culture affects its operations.

Although organizations may have different methods for establishing the right tone, a good starting point is to suggest a **code of ethics** or conduct and an anti-corruption policy endorsed by the board of directors or equivalent for public sector organizations. Once the board has clearly committed to a strong policy, the best approach is zero tolerance and full compliance with anti-corruption laws. This is not just ethically right; there also is increased pressure for compliance from legislative bodies and nongovernmental organizations. For example, securities or exchange regulations in certain

countries require listed companies to adopt a code of ethical conduct and even require the board to ensure compliance with the code.

Risk Appetite

Internal audit activity team members should understand the attitude and tolerance of the board and executive management toward corruption risks, assess whether that attitude is sufficiently restrictive, and validate that this attitude has been adequately communicated, ingrained, and managed throughout the organization. **Risk appetite** may by necessity be different from one geography or country to another. Internal auditors should keep in mind that any corruption which may exist in the country (or countries) in which their organization operates may create tension between the organization's values and the actions that must be taken to conduct business in that country.

If violations and legal consequences are present, indicating the organization's actual actions may run contrary to the stated risk appetite (e.g., zero tolerance), internal auditors may want to examine the reasons for the situation and subsequently report the matter or results to the board, executive management, and/or an appropriate oversight body.

Policies and Procedures

The organization's anti-corruption standards should be clearly defined in well-documented policies. Detailed underlying procedures should explain how employees, business partners, and third parties should behave, and clearly specify what behavior is unacceptable and noncompliant. Policies and procedures establish constraints and define and embed an organization's attitudes and practices on **fraud**, bribery, and corruption. The policies and procedures should include protocols for third-party dealings, payment processing, expense reporting, overall controls around financial books and records, training, and any specific jurisdictional requirements that may be relevant at a minimum. To safeguard against employee self-dealing, best practice policies also address conduct outside of the job and **conflicts of interest**.

Behavioral Interviewing

Behavioral interviewing techniques attempt to assess not only the subject's actions, but also to determine the motivations, beliefs, and underlying values that create the subconscious filter through which they make decisions.

Some organizations work with organizational psychologists and/or general psychologists to either perform the interviews and analysis of the data or to assist in the process.

Source: DeNederlandscheBank, *Supervision of Behaviour and Culture: Foundations, Practice & Future Developments,* 2015.

Communication and Training

Effective anti-corruption activities require careful and continuous communication and training, updated to align with changing regulations and evolving country norms. General training regarding what constitutes corruption, how it harms the organization, and how to report it should be provided to all members of the organization. In addition, customized training should be provided by function or job responsibility to address specific corruption risks. Additionally, some organizations may even require, as part of contractual and commercial relationships, or provide anti-corruption training to certain third parties and business partners.

As an extension of training and communication, self-certification activities may further reduce risk. For example, some organizations require management to periodically certify that they have not paid bribes and have no knowledge of other employees or service providers having done so. Some organizations require certain business partners to periodically provide similar certifications.

Investigations Protocols

Individuals at all levels should have support for resolving ethical dilemmas and making appropriate decisions. An accessible, anonymous whistleblower hotline for reporting suspected wrongdoing and seeking advice is crucial. Where local law permits, organizations also should offer a means to confidentially and/or anonymously report suspected corruption.

It is the responsibility of the board to ensure that the organization has an effective process for confidential investigation. A consistent investigative process including protocols for gathering and evaluating information, assessing potential wrongdoing, and administering penalties may help mitigate loss and manage risk.

Investigators should have the authority and skills to evaluate allegations and take appropriate action. If an in-depth investigation is deemed appropriate, investigators should first secure approvals, as needed, from senior management, the board, legal counsel, and other appropriate oversight bodies. In certain circumstances it also may be necessary to make public disclosures to law enforcement, regulators, shareholders, the media, or others; however, this should only be done by those individuals deemed authorized to do so on behalf of the organization.

Standard 2060 – Reporting to Senior Management and the Board states that "the **chief audit executive** must report periodically to senior management and the board on the internal audit activity's purpose, authority, and responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the *Standards*. Reporting must also include significant risk and control issues, including fraud risks, **governance** issues, and other matters that require the attention of senior management and/or the board." Therefore, reports also should include significant corruption risks and exposures, potential violations, and estimated impact.

There may be resistance to reporting corruption to the board. Management and legal counsel may downplay wrongdoing or may ask internal audit to delay reporting until corrective actions are taken. Internal auditors should clearly understand the board's communication requirements regarding corruption, including escalation, information type, and frequency. Standard 2600 – Communicating the Acceptance of Risks states, "When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board." As the interpretation of the standard reads, in part, "It is not the responsibility of the chief audit executive to resolve the risk."

Enforcement Standards

According to The IIA's Practice Guide, "Auditing Conduct Risk," "in terms of enforcement, internal auditors should examine whether 'punishments match the crime.' Management should strike a balance between being too lenient and too harsh. Examples of misconduct that must have zero tolerance because they are criminal acts and/or specifically prohibited by regulation include, for example, lying to customers or clients." The guide also states:

> Perhaps the most important question to ask is whether and how management is held accountable for both their personal actions and for the actions of people under their span of control. If conduct violations/issues are not linked to identifiable consequences, there is less incentive for employees to align activities to the organization's conduct rules. Unclear linkage of violations to consequences can also affect an organization's culture, as employees may see that not following the rules is acceptable.

Monitoring and Reporting

Reviews of key performance indicators (KPIs) and other metrics that are organizationally relevant can provide insight to how anti-corruption activities are working and which types of activities might affect levels of risk exposure. Some KPIs to consider are:

- Training completion rates.
- Complaints, their nature and resolution.
- Management overrides.
- Fraud occurrences and associated losses.
- Negative compensation changes resulting from conduct-related violations.
- Employee survey results.
- Client satisfaction survey results.
- Control environment survey results.

Internal auditors may continuously monitor these KPIs and other information to evaluate the effectiveness of the organization's anti-corruption activities, determine whether the time between risk occurrence and detection is acceptable (or increasing or decreasing), and monitor management's implementation of any corrective action plans.

Role of the Internal Audit Activity

Internal audit's role is not to develop and manage anti-corruption activities within their organization. However, internal auditors in organizations with informal anti-corruption activities may have the opportunity to help their organizations by identifying and investigating red flags in high-risk areas. Audit observations in these and other areas can be leveraged by the organization to prioritize its anti-corruption

> **Additional Resources**
>
> For more information on internal audit's role, see The IIA's practice guide "Engagement Planning Assessing Fraud Risks."

initiatives. Internal audit may also recommend implementing a formal program.

Internal auditors in organizations with formal anti-corruption activities/programs may have the opportunity to assess the effectiveness of each element and how all of a program's elements work together to prevent, detect, and correct actions that could lead to corruption.

IIA Standards 1210 – Proficiency, 1220 – Due Professional Care, and 2120 – Risk Management should also guide the role of internal audit in auditing anti-corruption activities.

Investigations

Internal audit's role in investigating corruption allegations depends on the internal audit activity's charter and resources and the organization's governance structure. Consideration should be given to factors such as the fraud, forensic, and IT skills among the activity's team members. Organizations may require corruption investigations to be conducted under the supervision of, and in coordination with, a special board committee, a regulatory body, the legal department, or another group.

The suspicion, discovery, and investigation of corruption are sensitive matters. Internal auditors should understand the cultural and legal landscape of the operational jurisdiction involved and be thoroughly familiar with local protocols for investigating and reporting. An organization may require that internal auditors obtain terms of reference such as the objectives, scope of work, activities, and tasks to be performed for investigations from those who called for one, or develop one (based on management briefing) and obtain management's approval before embarking on investigation. Additionally, internal audit should collaborate with the board and senior management to establish protocols for reporting suspected or actual incidents of corruption.

The need for an investigation may surface during the course of an engagement. If audit evidence indicates possible irregularities, internal auditors should:

- Follow the reporting protocol established by regulatory and/or organizational requirements and refer the matter to the investigatory group. If internal audit suspects that management is involved in the irregularity, it should find the appropriate party to whom it can report.
- Perform testing and document information, in conformance with Standard 2330 Documenting Information, to support the audit findings, conclusions, and recommendations.

If audit evidence points to an illegal act, internal auditors should seek legal advice directly or recommend that management do so. Internal audit should work with appropriate personnel, such as the fraud investigation unit, compliance function, legal counsel, and management (if possible, at a level above the parties involved in the act) to determine whether an irregularity or illegal act has occurred and to gauge its effect.

Alignment with and strict adherence to The IIA's Code of Ethics, particularly the attributes of Integrity and Competency, is vital for internal auditors in practice and appearance in every engagement and is especially relevant when they are called on to assess and report on the behavior of others.

Planning and Performing the Engagement

IIA Standards series 2200 and 2300 apply throughout this phase of an audit.

Gather Information

The chief audit executive, or internal auditors assigned by the CAE, should be involved as observers in various meetings throughout the organization regarding values and strategic planning. Internal auditors attending these meetings should be conscious of the information that pertains to or may affect anti-corruption activities. This information will also help internal auditors identify where risk information related to anti-corruption activities is retained in the organization.

While gathering information to understand the factors that are subject to an audit, internal auditors should also review prior assessments (e.g., risk assessments, reports by assurance and consulting service providers), process flows and controls, and interviews of relevant stakeholders. To identify key risks and controls for an anti-corruption activities assessment, internal auditors should have a thorough understanding of the way their organization sets, communicates, and expresses its values.

Documents internal auditors may want to review while gathering information include:

- Any value statements published by the organization; these may be labeled mission or vision statements or contained within such documents. Many times these are public and appear on the organization's website.
- Top-level, business-line level, and process-level strategies, objectives, and business plans.
- Risk appetite statements.
- Organization charts (high level and business units) and related reporting lines.
- Roles, responsibilities, and accountabilities of other control functions (e.g., compliance, risk management) and senior management.
- Governance framework.
- Tone at the top and leadership communications with employees.
- Approvals and selling processes related to products/services.
- Risk escalation protocols.
- Documentation of exceptions and management overrides.
- Codes of conduct/ethics including policies and procedures of speaking up, nonretaliation, and treating customers fairly.
- Ethics hotline information and training materials.
- Results of culture-related training and testing activities (e.g., sexual harassment, ethics, code of conduct).
- Employee survey results.
- Exit interview data.
- Minutes of meetings of board and relevant committees (e.g., governance, risk, nomination, remuneration, and ethics).
- Management's risk and control self-assessments (RCSAs) including management's action plans and their status.
- Relevant culture-related and risk management policies including incentives and compensation policy, requirements, reports, and expectations.
- Recruitment, onboarding, performance management, retention, and exiting processes.
- Status of issues raised by internal audit or other control functions, external auditors, and regulators, taking into consideration repeated and long outstanding issues and root causes that may be related to anti-corruption efforts.
- External auditor's report on the audited financial statements and letter of representation.
- Third-party management processes and assessments/audits.
- Fraud risk assessments and related results.
- Compilation of the laws and regulations that apply to the organization.

Some of these elements are public knowledge and can be obtained easily. Others will be more difficult and internal audit may have to work with available data to infer a conclusion.

Risk Assessment

Because any single internal audit engagement cannot cover every risk, internal auditors assess the significance of the risks identified by those in the second line (of the Three Lines model) or management during previous internal audit engagements and assessments performed by other internal or external entities or consultants, as described in Standard 2050 – Coordination and Reliance.[4]

Standard 2210 – Engagement Objectives states that objectives must be established for each engagement, and Standard 2210.A1 requires a preliminary assessment of the risks relevant to the activity under review. Internal auditors may interview relationship owners, business managers, procurement managers, legal personnel, and other relevant personnel with the technical knowledge to assist in identifying risks to the organization's anti-corruption activities.

The internal audit activity is responsible for assessing the quality of management's anti-corruption activities to determine whether the activities are adequate in design and/or operation. This is in accordance with Standard 2110.A1 that reads, "The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities." An assessment of the inherent risk of corruption in the organization's operations is warranted. When evaluating residual risk, management's anti-corruption activities should account for not only the financial, operational, and regulatory impact of corruption, but also nonfinancial impacts, such as damage to the organization's reputation or relationships with customers.

Even a small, contained corruption problem may have a damaging impact on an organization's reputation. Corruption can also have a negative impact on employee commitment, engagement, and the values they exhibit in their behavior. Some risks may appear insignificant on their own but

Residual Risk

Residual risk, or net risk, is the portion of inherent risk that remains after management executes its risk management strategies. With the help of management, internal auditors identify the risk management strategies and control processes and translate them into operational, or measurable, terms to help determine residual risk.

The CAE or assigned internal auditors should document the reasons for their determination of residual risk. This rationale lends support to internal audit's view of risk priorities, which is especially important in cases where internal audit judgement may be in conflict with a strict interpretation of risk rating results.

Source: Urton L. Anderson et al, *Internal Auditing: Assurance and Advisory Services*, 4th ed., 485.

---

4. The IIA's Three Lines Model: An update to the Three Lines of Defense, July 2020. https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf.

should be considered in the context of the organization's overall anti-corruption activities. As part of their assessment, internal auditors may wish to include risks that investigators would look for in a comprehensive, well-designed, and applied compliance and control program:

> For example, prosecutors should consider 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 results of this risk assessment will assist the CAE in determining the appropriate engagement approach, objectives, and scope. It will also assist the CAE in determining whether the resources available to the internal audit activity have the appropriate skills to be effective.

A sample list of risks, red flags, and audit considerations is provided in Appendix C, and a list of sample risk assessment questions is provided in Appendix D.

Planning the Engagement

Internal auditors should assess the effectiveness of anti-corruption activities to help anticipate the risk of potential incidents and identify whether any are occurring currently. This means paying attention to detective and corrective activities as well as preventive controls. Internal auditors may take many different approaches to auditing anti-corruption activities; this guide considers three:

1. Integrating anti-corruption elements into all engagements (integrated approach).
2. Selecting a set of key processes and controls related to anti-corruption activities, developing an engagement work plan, and performing targeted testing on the selected areas. This testing may be supplemented with interviews of a sample of employees in which auditors ask targeted questions to assess the effectiveness of anti-corruption activities (targeted approach).
3. Top-down assessments of anti-corruption efforts, which start with tone at the top and move down through all layers of the organization to individual employees (top-down approach).

Any of these approaches would allow internal auditors to develop a list of relevant anti-corruption risks and controls and map their audit results to those factors. Internal auditors may also evaluate corruption scenarios. These scenarios may be original, created by internal auditors based on corruption practices detected in the past, or constructed by the business or other relevant function

---

5. U.S. Department of Justice, Criminal Division, "Evaluation of corporate compliance programs," June 2020, https://www.justice.gov/criminal-fraud/page/file/937501/download.

(e.g., compliance), or a combination of these. This work may allow internal auditors to spot trends or common themes that could be presented to senior management and the board.

Coordination and Reliance

Auditing anti-corruption activities requires varying levels of collaboration and information sharing with other governance functions — such as regulatory compliance, external auditors, investigators, and the governing board — as discussed in the Three Lines model and in Standard 2050 – Coordination and Reliance. Before getting started, the CAE or lead internal auditor should consult with the organization's general counsel or legal representative to gain a full understanding of potential legal implications of the audit scope, fieldwork, and findings.

Internal audit may share information and work with other functions such as fraud investigation, legal counsel, compliance, and others. For example, South Africa's King Report and King Code of Corporate Governance makes this explicit by stating that the board should ensure there is an effective risk-based internal audit function that can be a source of information about instances of fraud, corruption, unethical behavior, and other irregularities. Also, in some countries, information on irregularities and illegal acts is required to be exchanged with regulatory agencies.

Engagement Resource Allocation

Those assigned to anti-corruption audit engagements need certain skills. In conformance with Standard 2230 – Engagement Resource Allocation, the CAE should assess the skills of internal audit team members to ensure that the internal audit activity has the appropriate skills to provide meaningful information and insight to management on culture-related risks.

If work regarding anti-corruption is performed by another assurance provider and used by the internal audit activity, the CAE should also confirm the work is objective and thorough. As noted in Standard 2050 – Coordination and Reliance, the CAE should carefully consider the competency, objectivity, and due professional care of other providers and should clearly understand the scope, objectives, and results of their work. Responsibility for ensuring adequate support exists for the conclusions and opinions reached by the internal audit activity rests with the CAE.

Documenting Information

During planning, internal auditors document information in engagement workpapers according to Standard 2330 – Documenting Information. This information becomes part of the engagement work program that must be established to achieve the engagement objectives, as required by Standard 2240 – Engagement Work Program.

The process of establishing the engagement objectives and scope may produce any or all of these types of workpapers:

- Process maps.
- Summary of interviews.

- Preliminary risk assessment (e.g., risk and control matrix and heat map).
- Rationale for decisions regarding which risks to include in the engagement.
- Criteria that will be used to evaluate the area or process under review (required for assurance engagements, according to Standard 2210.A3).

Performing the Engagement

Whether internal auditors take the approach of auditing each element of an organization's anti-corruption activities individually or incorporating an assessment of anti-corruption activities in all engagements, this guide reviews audit considerations for each element to satisfy Standard 2300 – Performing the Engagement. Internal auditors may choose which considerations would be appropriate to the approach they are taking.

Tone at the Top

Ideally, senior management and the board work together to define the organization's values and proactively emphasize and model those values, ensure strategies are consistent with the values, and hold management accountable to execute their duties within the organization's risk appetite. Internal auditors may test the existence and effectiveness of the tone at the top in their organization by:

- Evaluating the existence of a code of conduct and an anti-corruption policy endorsed by the board of directors and signed off by all employees annually.
- Evaluating whether the financial and performance results communicated at regularly scheduled corporate meetings (e.g., investors' calls) are congruent with those communicated internally among employees.
- Reviewing whether senior management's presentations to employees (or minutes of staff meetings) include slides/information on the organization's desired culture and "doing the right thing."
- Assessing the nature and frequency of board and senior management's internal and external communications to convey the "right" tone at the top.
- Reviewing the results of employee surveys paying particular attention to the questions related to ethical behavior, organizational culture, management expectations, tone at the top, and responses to open-ended questions.
- Reviewing comments obtained in recent exit interviews and any action plans that may have resulted.
- Reviewing the availability and use of ethics/whistleblower hotlines (or other reporting mechanisms) and the disposition of reports to the hotline(s) and of any investigations triggered by those reports.
- Reviewing the minutes of audit committee and board meetings.

- Attending audit committee and board meetings to observe and assess the messages conveyed between members and to management.

In addition, internal auditors may wish to ask these questions:

- Is the organization aware of its exposure to global corruption risks?
- Do employees periodically certify that they are compliant with anti-corruption standards and the organization's code of conduct and attest that they have no knowledge of any incidence of bribery or corruption?

Policies and Procedures

Organizations should establish policies and procedures that clearly define anti-corruption standards, controls, and expectations to ensure employees are aware of and can execute business processes in line with those expectations. Internal auditors should verify that policies and procedures are:

- Documented, easily accessible, and updated periodically.
- Approved by appropriate management or the board.
- Compliant with applicable laws and regulations.

In addition, internal auditors may consider asking these questions:

- Do the anti-corruption policies and procedures comply with applicable laws and regulations?
- Do policies and procedures address gifts, entertainment, meals, travel expenses, charitable donations, and facilitation payments?
- Do general policies and procedures for areas such as sales, purchases, rewards and recognition, etc., properly include the organization's anti-corruption policies?
- Do employees fully understand the organization's principal anti-corruption policies?
- Have the policies been operationalized?

Communication and Training

There can be a gap between the perception of corruption risks on the ground, where an event would likely occur, and the more distant view at the board level. This is especially true if effective risk assessments, analyses, and communication are lacking. In the constantly changing world of anti-corruption laws and regulations, communication and training from the top of the organization through all employment levels is critical. At a minimum, internal auditors should review:

- Rates of completion and pass rates for training programs including ethics, code of conduct, core values, etc.

- Nature, type, and frequency of training provided (e.g., general or tailored or both, annual or periodic, web-based or in person or both, language(s) available if applicable for the organization).
- Any measures to assess the effectiveness of training (e.g., evaluation of impact on employee behavior, lessons learned incorporated into training).

In addition, internal auditors may consider asking these questions:

- Is anti-corruption training mandatory for all employees?
- Is training and communication tailored to the geographical region, function, and job responsibility?
- Do employees understand how violations of the anti-corruption program may impact salary, promotion, and continued employment?

Information on auditing ethics and whistleblower programs is provided in Appendix F.

Investigatory Processes

To investigate cases of potential corruption, organizations should have a defined process that includes multiple organizational disciplines and may require a team of subject matter experts, if such people are available to the organization. In some organizations, internal auditors may be tasked with a role in investigations. Per Standard 1210 – Proficiency, internal auditors must possess the competencies needed to perform their individual responsibilities.

Additionally, per Standard 1130 – Impairments to Independence or Objectivity, internal auditors who participate in investigations must disclose to appropriate parties any potential impairments to independence or objectivity that could affect their participation in future internal audit engagements.

At a minimum, internal auditors should confirm that the people involved in investigations have the appropriate skills and are following the organization's investigation protocols, policies, and procedures.

In addition, internal auditors may consider asking these questions:

- Does the organization have formal, defined processes and protocols for investigating alleged corruption?
- Should investigations be conducted with legal oversight due to the sensitive nature of topics at issue and/or the requirement of the application of legal standards?
- Do the persons responsible for investigations have the requisite skills, experience, objectivity, autonomy, and organizational independence?
- Do the persons responsible for investigations have the right resources and access to data to perform their job?

- Does the organization monitor, track, and analyze the timing responsiveness between the initiation of an investigation and its resolution and disposition?
- How does the organization incorporate investigation results into its policies and operations?

Enforcement Standards

Ideally, enforcement standards for anti-corruption activities should be consistent, comply with legal requirements, and be applied fairly across the organization. While it may seem that this would be a difficult concept to test, there are measurable ways to obtain information that may allow internal auditors to evaluate the effectiveness of an organization's enforcement actions including:

- Examining a sample of incidents that should have resulted in disciplinary action or compensation impact for the effectiveness of related processes.
- Examining the communication activities of management regarding reportable incidents.
- Auditing the organization's whistleblowing and complaint handling procedures.
- Confirming the organization is following regulatory and internal requirements related to conduct that impact compensation.
- Confirming that individual processes where conflicts of interest or segregation of duties violations may occur are adequately structured and monitored to avoid these risks.

In addition, internal auditors may consider asking these questions:

- Do employees and third-party providers (e.g., agents, sales consultants, distributors, and vendors) comply with the organization's code of conduct regarding corruption?
- Are cases of bribery or corruption evaluated objectively and disciplinary actions consistently implemented in accordance with policy?

Monitoring and Reporting

Organizations should establish effective monitoring systems that provide senior management and the board with periodic updates. Reporting systems should also extend to external authorities who may require self-reporting of any incidents. While internal auditors should be aware of management's reporting systems and periodically evaluate whether they are operating appropriately, the internal audit activity should not supplant management's monitoring role.

In addition, internal auditors may consider asking these questions:

- Does the organization have a formal process for monitoring the effectiveness of its anti-corruption activities?
  - o Is this process established to ensure objectivity?
  - o Is this process implemented properly?

- What controls are in place to respond to corruption matters before they become significant issues?
- Does the organization have defined protocols for reporting alleged or confirmed bribery or corruption to the board or other authority?
- Is the board regularly informed about whistleblower complaints received, investigations in progress, and investigations closed?

Communicating Internal Audit Results

Standard 2400 – Communicating Results is self-explanatory in that results of an engagement must be communicated. According to the interpretation of Standard 2410 – Criteria for Communicating, "Opinions at the engagement level may be ratings, conclusions, or other descriptions of the results. Such an engagement may be in relation to controls around a specific process, risk, or business unit. The formulation of such opinions requires consideration of the engagement results and their significance."

CAEs should be aware that a specific reporting format is not required by the *Standards*. Not all internal audit reports must be written or include ratings. Alternatives to a traditional report may be considered specifically for issues of corruption. Reporting on these issues may be sensitive, but the CAE has a responsibility to openly communicate to senior management and the board.

An organization's anti-corruption activities can be a compilation of intangible, fluid actions, and the CAE must be free to communicate issues that may not rise to the level of a formal control deficiency/recommendation, in addition to any formal, written recommendations identified.

Appendix A. Relevant IIA Standards and Guidance

The following resources were referenced throughout this practice guide. For more information about applying The IIA's *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Code of Ethics
Principle 1: Integrity
Principle 2: Objectivity
Principle 3: Confidentiality
Principle 4: Competency

Standards
Standard 1130 – Impairment to Independence and Objectivity
Standard 1210 – Proficiency
Standard 1220 – Due Professional Care
Standard 2050 – Coordination and Reliance
Standard 2060 – Reporting to Senior Management and the Board
Standard 2110 – Governance
Standard 2120 – Risk Management
Standard 2200 – Engagement Planning
Standard 2210 – Engagement Objectives
Standard 2230 – Engagement Resource Allocation
Standard 2240 – Engagement Work Program
Standard 2300 – Performing the Engagement
Standard 2330 – Documenting Information
Standard 2400 – Communicating Results
Standard 2410 – Criteria for Communicating
Standard 2600 – Communicating the Acceptance of Risks

Guidance and Other IIA Resources
Practice Guide, "Auditing Conduct Risks," 2020
Practice Guide, "Auditing Culture," 2019
Practice Guide, "Engagement Planning: Assessing Fraud Risks," 2017
Position Paper, "The IIA's Three Lines Model: an Update of the Three Lines of Defense," 2020
Internal Audit Foundation: "Auditing Anti-Bribery Programs," 2018

Appendix B. Glossary

Terms identified with an asterisk are taken from The IIA's *International Professional Practices Framework* "Glossary," 2017 edition.

board* – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

chief audit executive* – Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

code of ethics* – The Code of Ethics of The Institute of Internal Auditors are Principles relevant to the profession and practice of internal auditing, and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.

compliance* – Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements**.**

conflict of interest* – Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

corruption – Acts in which individuals wrongfully use their influence in a business transaction to procure some benefit for themselves or another person, contrary to their duty to their employer or the rights of another (for example, kickbacks, self-dealing, or conflicts of interest).[6]

fraud* – Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

---

6. Urton L. Anderson, et al., *Internal Auditing: Assurance and Advisory Services*, 4th ed., BM-11.

governance* – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

internal audit activity* – A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

risk* – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

risk appetite* – The level of risk an organization is willing to accept.

Appendix C. Risks, Red Flags, and Audit Considerations

High-risk areas for corruption include geography and industry; hiring/employment (including internships); third-party/vendor management; gifts, entertainment, and charitable or political contributions; social responsibility programs; procurement; sales; finance; IT; upper management; and government relations. These risks, their descriptions, accompanying red flags, and potential audit considerations are presented here.

RISK: GEOGRAPHY AND INDUSTRY

Risk Description

Some countries or jurisdictions where organizations operate in cash-based economies have a higher incidence of corruption. The local regulatory environment also impacts risks. Similarly, certain industries (e.g., construction/infrastructure) are more susceptible to corruption. It also is important to consider the respective industries of business partners and third-party relationships.

Through globalization, joint ventures, and partnerships, organizations may set up operations in parts of the world where the ethical environment differs from that of the home country or where the culture includes acts that would be considered bribery as an acceptable way to facilitate business. Risks may be compounded if anti-corruption policies are not clear, detailed, translated into local languages, and relevant to regional business practices.

Red Flags

- Operations in countries with a reputation for higher risk of bribery or corruption.
- Activities with industries or specific organization's that have a reputation for a higher risk of bribery or corruption.

Audit Considerations

- Where a culture of corruption exists, internal auditors of the parent organization should evaluate each situation, including those under joint venture/partnership, and discuss dilemmas with the board.
- When senior management does not support a bribery policy and the organization is operating in a culture where corruption are common, the line between what is and is not acceptable is likely to be blurred. The internal auditor should evaluate acts and actions against the organization's policy regardless of the apparent permissiveness of a particular environment.
- Evaluate the organization's compliance risk assessment process and results. The internal auditor should pay attention on how the organization identifies, analyses and addresses risk and allocates resources to high-risk areas and prioritizes action plans.

RISK: HIRING AND EMPLOYMENT

Risk Description

The hiring process, including candidate background checks, is an important consideration for potential corruption. This is especially true in cases of mergers and acquisitions.

Red Flags

- Hiring employees with a history of wrongdoing.
- Hiring employees with connections to other employees or to government officials.
- Employees without required qualifications for position.
- Phantom employees.

Audit Considerations

- Review effectiveness of policies and practices for confirming that personnel considered for employment in roles vulnerable to bribery do not have a history of wrongdoing.
- Confirm existence of employees in the country/location.
- Verify validity of employees.
- Compare job descriptions (particularly requirements or specific qualifications needed) against employee's resume or CV.

RISK: THIRD PARTIES

Risk Description

Relationships with vendors, agents, lobbyists, contract employees, distributors, consultants (e.g., business development), and other intermediaries such as customs agents, brokers or freight forwarders can be exploited by corruption, especially bribery schemes. Corruption can occur on the part of the organization hiring the third party and within the third party itself. Corruption in an organization's third-party risk management framework and processes can expose the organization to compliance, financial, and reputational risks.

Red Flags

- Inadequate third-party management procedures (e.g., lack or no due diligence requirements, documentation available to support due diligence results).
- Unproductive or suspicious interviews with employees, agents, and contractors.
- Close personal or familial relationships between employees and vendors.
- Lack of competitive bid processes for vendors or customers.
- Use of agents or third parties to pay bribes.
- The existence of fictitious suppliers.
- Inappropriate acceptance of gifts, money, or entertainment expense payments in return for preferential treatment to providers bidding for goods and services.
- Conflicts of interest among members of assessment panels (for large procurements) and vendors submitting the bids, including vendors related to government officials.
- Purchasing in installments with the same supplier (i.e., provider) to avoid the organization's authorization levels and spending limits (structuring).
- Extending contracts for excessive periods of time without "testing the market" for better terms.
- Making a high-value purchase with a unique or exclusive supplier.
- Purchasing goods inconsistent with business needs, including overpaying for services and products.
- Inadequate spend data and vendor data or inconsistent data across procurement related systems.

- Use of sole-sourced vendors not properly vetted, including low compliance with corporate preferred buying guidelines.
- Inappropriate vendor creation and management and multiple appearances of the same vendor within the master file.
- Duplicate payments.
- Limited segregation of duties involving payments, credits, and reconciliation of vendors and suppliers.

Audit Considerations

- Review agent and other third-party selection and screening processes and due diligence practices.
- Review practices for staying current on third-party ownership and merger and acquisition activity as well as sanctions and debarments.
- Review policies for hiring and retaining agents and contractors and training them in anti-corruption activities.
- Ensure that contracts specify the expectation of compliance with the code of conduct and anti-corruption regulations.
- Review contracts to ensure the existence of right-to-audit clauses.
- Review expenses reimbursed to third parties. Interview third-party employees.
- Evaluate use of agents and other third parties, considering reasonableness and necessity (i.e., whether it is reasonable to use the third party chosen for the specific task).
- Review controls over supplier selection and vendor setup.
- Review vendor setup in the payment system.
- Review the competitive bid process and documented results for certain awarding determinations.
- Test that goods and services are real and at market prices.
- Conduct supplier visits and interview suppliers.
- Validate vendor addresses.
- Validate vendor companies via publicly available records.
- Analyze vendor locations and locations of vendor bank accounts for reasonableness (e.g., vendors located in places with no known organizational locations or bank accounts set up in certain "risk" locations).
- Compare employee data to business partners master file data (e.g., fuzzy logic around names, addresses, and telephone numbers).
- Analyze payment data using Benford's Law.
- Visualize payment data and correlate against operations timing and location.

RISK: GIFTS AND ENTERTAINMENT

Risk Description

Travel, entertainment, and gifts given or received by the organization or the organization's employees can be methods of bribery. Any act or gift that may have the capacity to influence business decisions in an illegal way must be considered a risk and should be limited in accordance with organizational policy requirements. In the public sector, organizations should be particularly careful interacting with government officials. These may include politicians, elected officials, judges, arbitrators, mediators, officers and employees of political parties; officers and employees of government authorities, departments or public organizations or enterprises; and officers and employees of entities that are government owned or controlled. Individuals that act in an official capacity for governments or public organizations are also government officials.

Red Flags

- Excessive travel and entertainment expenses, especially for entertaining government officials.
- Frequent or excessive entertainment and gifts provided to customers, suppliers, or government officials.
- Frequent or excessive charitable and political donations.

- Inadequate or vague gift/hospitality/entertainment policies and/or guidelines.
- Unusual or unsupported social responsibility programs.

Audit Considerations

- Review appropriateness of entertainment and gift policies.
- Review payments related to travel, entertainment, and gifts.
- Review approvals required for giving gifts.
- Perform keyword searches on travel and expense reports for inappropriate travel/gifts.
- Review compliance with the charitable donations policy.
- Review payments to charitable and political organizations.
- Consider relationships between charities and other parties (e.g., government officials and organization management).
- Confirm charities are bona fide organizations.

RISK: FINANCE AND ACCOUNTING

Risk Description

Most bribery involves disbursement of cash and the recording of that disbursement in the financial records.

Red Flags

- Payments of cash to facilitate deals and transactions.
- Lack of supporting documentation for cash transactions.
- Lack of appropriate segregation of duties for control of cash, nonroutine payments, or other transactions.
- Lack of, or poor supporting documentation for, expense reports.
- Cash used to pay bribes.
- The existence of off-balance-sheet bank accounts.
- Credit notes and rebates used as a method to pay bribes.
- Bookkeeping records insufficient to identify bribery schemes.
- Increasing or frequent write-offs of accounts receivable.
- Limited segregation of duties involving payments, credits, and reconciliation of vendors and suppliers.
- Payments or transactions classified or labelled as miscellaneous, other, sundry, generic, or other similar type of wording.

Audit Considerations

- Review end-to-end expense processing for check/ wire/electronic funds transfer, petty cash, employee payroll, and employee expense reimbursement.
- Review controls to establish bank accounts and signature authorities.
- Review bank reconciliation controls and performance of monthly reconciliations.
- Review controls over petty cash.
- Review travel and entertainment payments and reimbursements, as these are common methods of bribery.
- Review financial information, detailed accounts, bank accounts, and payment records to identify any off-balance-sheet accounts usable for bribery purposes.
- Review controls and test transactions related to credit notes and rebates.
- Confirm that the nature and amount of credit notes and rebates are consistent with business practices.
- Review accounting policies and practices to assess regulatory compliance.
- Reconcile balances between subledger and general ledger.

- Perform keyword searches or develop word clouds and verify validity of transactions meeting certain criteria.
- Evaluate accounts to determine if parallel books are maintained in certain countries to disguise illegal or irregular transactions.
- Review and test IT access controls related to vendor management, accounts payable, and accounts receivable.
- Test transaction level controls for segregation of duties.

Appendix D. Sample Risk Assessment Questions

This list represents some questions that may be asked during a risk assessment. It is not intended as an audit program or an exhaustive list of questions that may be relevant.

1. Does the organization use business intelligence resources to identify corruption risks when exploring business opportunities in established and emerging markets?

2. Does the organization's due diligence process meet regulatory requirements for scope and thoroughness?

3. Does the organization's due diligence process extend to hiring practices and third-party providers?

4. Is there a history of lawsuits, fines, and penalties related to corruption?

5. Are measures in place adequate to reduce possibilities and motivation for corrupt behavior?

6. What methodology has the company used to identify, analyze, and address the particular risks it faces?

7. What information or metrics has the company collected and used to help detect the type of misconduct in question?

8. Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas such questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors?

9. Does the company give greater scrutiny, as warranted, to high-risk transactions than more modest and routine hospitality and entertainment?

10. Is the risk assessment current and subject to periodic review?

Source: U.S. Department of Justice, Criminal Division, "Evaluation of Corporate Compliance Programs," June 2020, https://www.justice.gov/criminal-fraud/page/file/937501/download.

Appendix E. Sanctions

Sanctions are imposed by numerous countries and bodies and can have an impact on operations and conduct globally in a variety of contexts. Breaching sanctions can result in civil, criminal, and regulatory liability resulting in substantial fines and reputational damage.

Many countries follow the sanctions regimes enacted by the United Nations Security Council (UNSC). The UNSC has enacted sanctions in a variety of forms to meet different objectives. Some involve comprehensive economic and trade sanctions. More targeted approaches include arms embargoes, travel bans, and specific financial or commodity restrictions. Sanctions may cover individual persons, political or military organizations, companies, products, and even individual transactions. Sanctions may be in effect in only part of a geographical area or country, leaving the rest of the country open for business. The UNSC endeavors to keep its sanctions regimes targeted to promote peaceful political transitions, reign in government actions that contravene a country's constitution, constrain terrorism, protect human rights, and promote nonproliferation of weapons of mass destruction. Their sanctions regime is closely coordinated with their peacekeeping activities.

Internal auditors should be aware of sanctions that may affect the organization's operations. As noted previously, many countries' laws enable them to prosecute corruption and sanctions violations wherever they occur. Sanctions are fluid in today's ever-changing geopolitical environment, so internal auditors should rely on legal counsel and other subject matter experts to assist them when evaluating this area.

United Nations Security Council

The Security Council can take action to maintain or restore international peace and security under Chapter VII of the United Nations Charter.

Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force.

Since 1966, the Security Council has established 30 sanctions regimes, in Southern Rhodesia, South Africa, the former Yugoslavia (2), Haiti, Iraq (2), Angola, Rwanda, Sierra Leone, Somalia and Eritrea, Eritrea and Ethiopia, Liberia (3), Democratic Republic of Congo, Côte d'Ivoire, Sudan, Lebanon, Democratic People's Republic of Korea, Iran, Libya (2), Guinea-Bissau, Central African Republic, Yemen, South Sudan and Mali, as well as against Islamic State of Iraq and the Levant (Da'esh) and Al-Qaida, and the Taliban.

Source: Sanctions, "2021 Fact Sheets: Subsidiary Organs of the United Nations Security Council," https://www.un.org/securitycouncil/sanctions/information#:~:text=Since%201966%2C%20the%20Security%20Council,%2C%20Guinea%2DBissau%2C%20CAR%2C.

Appendix F. Auditing Ethics Programs and Whistleblowing/Complaint Processes

In accordance with Standard 2110.A1, internal audit's primary objective is to evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities. Ethics programs and whistleblowing/complaints processes should be audited regularly to ensure they are updated in a reasonable manner, understood by all employees, and effective.

Engagement to Assess Ethics Programs and Codes of Conduct

Internal auditors may review:

- The process(es) used to develop and/or update the organization's ethics program and code of conduct including:
    - Subject matter coverage is reviewed and updated according to good practices.
    - Appropriate parties are included in the review process.
    - Input is obtained from the board and executive management.
    - Input from related committees (ethics, risk, compensation, etc.) is considered.
    - Audit committee review and approval is documented and validated.

- Documentation demonstrating whether ethics-related complaints, whistleblowing situations, or other incidents involving management as individuals or as a group are investigated and addressed promptly and in a manner consistent with the organization's ethics policies, escalation protocols, code of conduct, etc.
    - Is there evidence of management or other employees retaliating against those who report issues?
    - Is there a statistical trend of complaints, whistleblowing situations, or other incidents, which could indicate that the controls in place are not effective?

- Rates of completion and pass rates for electronic training programs including ethics, code of conduct, core values, etc.

Engagement to Assess Whistleblowing/Complaints

Questions to ask may include:

- Are questionable issues reported?
- If issues are reported, is there a defined escalation protocol depending on the type of issue (ethics, sexual harassment, etc.)?
- Are issues escalated according to an established protocol?

- Is there a "speak up" culture that makes employees comfortable escalating issues that may occur on any level of the organization?

- If an organization's policy provides for protections and rewards for whistleblowers (assuming reported issues that have escalated and been handled through appropriate channels have merit and result in a settlement that may reward the whistleblower), do appropriate internal controls exist to ensure follow through?

- Are there any applicable laws that may affect an organization's ethics and whistleblowing programs in locations in which the organization does business?

Hotline Vendors

As the exposure of corruption has grown in recent years, whistleblower hotlines and similar reporting tools have become critical to organizational governance. Third-party vendors that provide ethics or whistleblowing hotlines may be cost effective alternatives to monitoring hotlines within the organization but should be considered carefully. Even with a vendor accepting hotline calls, the organization must manage the response. The challenge remains to make the hotline operation an integral element of any organization's risk management, compliance, and ethics program. Once established, the hotline program should operate under strict policies and procedures. To do otherwise invites increased exposure to liability and unwanted consequences.

Appendix G. Global Anti-corruption and Anti-bribery Resources

These lists provide some global and regional resources but are not exhaustive. Internal auditors should check with their organization's legal and/or compliance personnel for assistance and may also consider researching additional global and regional resources in locations where their organization operates.

Global Resources

"Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents," OECD, https://www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf.

Global Compliance News, https://globalcompliancenews.com/anti-corruption/anti-corruption-laws-around-the-world/.

Inter-American Development Bank, https://www.iadb.org/en/integrity/international-anti-corruption-events.

International Organization for Standardization, ISO 37001, https://www.iso.org/iso-37001-anti-bribery-management.html.

Organisation for Economic Co-operation and Development, www.oecd.org.

Transparency International, www.transparency.org.

United Nations Convention Against Corruption, https://www.unodc.org/unodc/en/treaties/CAC/.

United Nations Office on Drugs and Crime, www.unodc.org.

United Nations Global Compact, www.unglobalcompact.org.

World Bank Group, Integrity Vice Presidency, https://www.worldbank.org/en/about/unit/integrity-vice-presidency.

World Bank Group, "Combatting Corruption," https://www.worldbank.org/en/topic/governance/brief/anti-corruption.

World Economic Forum, Partnering Against Corruption Initiative, https://www.weforum.org/communities/partnering-against-corruption-initiative.

Regional Resources

Africa: African Union Convention on Preventing and Combating Corruption, https://au.int/en/treaties/african-union-convention-preventing-and-combating-corruption.

Australia: Anti-Corruption, https://www.ag.gov.au/integrity/anti-corruption.

Australia: Standards Australia, https://infostore.saiglobal.com/en-us/standards/DR-AS-8001-2020-1189365_SAIG_AS_AS_2843880/.

China: Anti-Corruption in China, translated by *Global Compliance News*, https://globalcompliancenews.com/anti-corruption/handbook/anti-corruption-in-china/#:~:text=Under%20Articles%20389%2C%20390%2C%20390A,for%20the%20purpose%20of%20securing.

European Union: European Union Anti-Corruption Initiative, https://euaci.eu/.

Hong Kong: Independent Commission Against Corruption, https://www.icac.org.hk/en/law/law/index.html.

India: Key Amendment to India's Anti-Corruption Legislation Has Significant Implications for Multinationals Doing Business in India, translated by Ropes & Gray LLP, https://www.ropesgray.com/en/newsroom/alerts/2018/08/Key-Amendment-to-Indias-Anti-Corruption-Legislation-has-Significant-Implications-for-Multinationals.

Indonesia: Corruption Eradication Commission, https://www.acauthorities.org/country/id; "Good Governance and the Rule of Law in Indonesia" (blog entry), https://resourcegovernance.org/blog/good-governance-and-rule-law-indonesia; "Indonesia Corruption Report" (blog entry), https://www.ganintegrity.com/portal/country-profiles/indonesia/.

Japan: National Public Service Ethics Act, translated by *Japanese Law Translation*, http://www.japaneselawtranslation.go.jp/law/detail_main?re=01&vm=02&id=2952.

Japan: Unfair Competition Prevention Act No. 47 of 1993, translated by *Japanese Law Translation*, http://www.japaneselawtranslation.go.jp/law/detail/?ky=%E7%99%BB%E8%A8%98&page=4&re=01.

Latin America: OECD Latin American and Caribbean Anti-Corruption Initiative, https://www.oecd.org/daf/anti-bribery/anti-briberyconvention/oecd-latinamericaanti-corruptionprogramme.htm.

Peru: Lima Commitment "Democratic Governance against Corruption," https://www.state.gov/lima-commitment-eighth-summit-of-the-americas/.

Singapore: The Prevention of Corruption Act, https://sso.agc.gov.sg/Act/PCA1960; Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act, https://sso.agc.gov.sg/Act/CDTOSCCBA1992.

United Kingdom: Anti-bribery Policy, https://www.gov.uk/anti-bribery-policy.

United States: Foreign Corrupt Practices Act, https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

Appendix H. References and Additional Resources

References

Anderson, Urton L., Michael J. Head, Sridhar Ramamoorti, Cris Riddle, Mark Salamasick, and Paul J. Sobel. *Internal Auditing: Assurance and Advisory Services, 4th ed*. Lake Mary, FL: Internal Audit Foundation. 2017. https://bookstore.theiia.org/internal-auditing-assurance-advisory-services-fourth-edition-2.

Organisation for Economic Co-operation and Development. "OECD Work on Anti-corruption and Integrity." Accessed February 12, 2021. https://www.oecd.org/corruption-integrity/about/.

Raaijmakers, Mirea, Wieke Scholten, Mélanie Rouppe van der Voort, Anousha Wajer, Wijnand H.J.M. Nujits, Moritz Römer, Jildau Piena, Melanie de Waal, and Ingeborg Rademakers. *Supervision of Behaviour and Culture: Foundations, Practice & Future Developments*. DeNederlandscheBank, Eurosysteem. Netherlands: DNB Repro & Post Department, 2015. https://www.dnb.nl/media/1gmkp1vk/supervision-of-behaviour-and-culture_tcm46-380398-1.pdf.

The Institute of Internal Auditors. "The IIA's Position Paper: The Three Lines Model: an Update of the Three Lines of Defense." Lake Mary, FL, 2020. https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Three-Lines-Model-Updated.pdf.

Transparency International. *Corruption Perceptions Index* 2020. Berlin, 2021. https://www.transparency.org/en/cpi/%202015/index/nzl.

Additional Reading

American Center for Government Auditing. "Audit Focus: Organizational Helplines and Hotlines." The IIA, 2017. https://dl.theiia.org/ACGAMember/ACGA-Audit-Focus-Organizational-Helplines-and-Hotlines.pdf.

Cohn, Alain, Ernst Fehr, and Michel André Maréchal. "Business Culture and Dishonesty in the Banking Industry." *Nature* 516, 86–89 (2014). https://doi.org/10.1038/nature13977.

Cressey, Donald R. "The Criminal Violation of Financial Trust." *American Sociological Review* 15, no. 6 (1950): 738-43. Accessed January 26, 2021. http://www.jstor.org/stable/2086606.

Fountain, Lynn. *Raise the Red Flag: An Internal Auditor's Guide to Detect and Prevent Fraud*. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation, 2015. https://bookstore.theiia.org/raise-the-red-flag-an-internal-auditors-guide-to-detect-and-prevent-fraud.

Jex, Susan, and Eddie J. Best. *A Journey Into Auditing Culture: A Story and a Practical Guide*. Lake Mary, FL: Internal Audit Foundation and Grant Thornton – United Kingdom, 2019. https://bookstore.theiia.org/a-journey-into-auditing-culture.

Kusserow, Richard P. "Auditing Hotline Effectiveness." Strategic Management Services website, June 2013. https://www.compliance.com/resources/auditing-hotline-effectiveness/.

Sartor, Michael A. and Paul M. Beamish. April 4, 2019. "Private Sector Corruption, Public Sector Corruption and the Organizational Structure of Foreign Subsidiaries." *Journal of Business Ethics* 167 (2020): 725-744. https://doi.org/10.1007/s10551-019-04148-1.

St-Onge, Elizabeth, Ege Gürdeniz, and Elena Belov. "Measuring Conduct and Culture: A How-To Guide for Executives." New York: Oliver Wyman, 2018. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/april/Conduct_and_Culture_Measurement_Oliver_Wyman.pdf.

United Nations Office on Drugs and Crime. *Reporting on Corruption: A Resource Tool for Governments and Journalists*. New York: United Nations, 2014. http://www.unodc.org/documents/congress/background-information/Corruption/Resource_Tool_for_Governments_and_Journalists.pdf.

The Institute of Internal Auditors. "A Conspiracy of Silence?" *Tone at the Top,* issue no. 88 (August 2018). https://dl.theiia.org/AECPublic/Tone-at-the-Top-August-2018.pdf.

The Institute of Internal Auditors. "More Than Just Setting the Tone: A Look at Organizational Culture." *Tone at the Top*, issue no. 76 (February 2016). https://dl.theiia.org/AECPublic/Tone-at-the-Top-February-2016.pdf.

Acknowledgements

Guidance Development Team

Jose Esposito, CIA, CRMA, Peru (Chairman)
Teis Stokka, CIA, CRMA, Norway (Lead)
Ching-Shin Chou, CIA, CCSA, CRMA, CGAP, China
David Dominguez, CIA, CRMA, United States
James Enstrom, CIA, United States
Hazem Keshk, CIA, CRMA, Egypt
Catherine Melvin, CIA, United States
Keri Rogers, CIA, CRMA, United States
Peter Stokhof, CIA, CCSA, France

Contributors

Mohammed Abdullah, Egypt
Anna Erasmus, CIA, CCSA, CRMA, South Africa
Chris Kisuuki, United States
Cornelius Klumper, CIA, United States

IIA Global Standards and Guidance

Harold Silverman, CIA, QIAL, CRMA, Managing Director
Anne Mercer, CIA, CFSA, Director
David Petrisky, IT Director
Dan Walker, CIA, FS Director
Pam Stroebel Powers, CIA, CRMA, Public Sector Director
Shelli Browning, Technical Editor
Lauressa Nelson, Senior Editor
Christine Janesko, Content Developer and Technical Editor
Geoffrey Nordhoff, Content Developer and Technical Editor

The IIA would like to thank the following oversight bodies for their support: Professional Guidance Advisory Council, Financial Services Guidance Committee, Guidance Development Committee, Information Technology Guidance Committee, Public Sector Guidance Committee, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and the International Professional Practices Framework Oversight Council.