UNODC
United Nations Office on Drugs and Crime

STATE OF INTEGRITY

A GUIDE ON CONDUCTING CORRUPTION RISK ASSESSMENTS IN PUBLIC ORGANIZATIONS

UNITED NATIONS OFFICE ON DRUGS AND CRIME

STATE OF INTEGRITY

A GUIDE ON CONDUCTING CORRUPTION RISK ASSESSMENTS IN PUBLIC ORGANIZATIONS

UNITED NATIONS
Vienna, 2020

This publication has not been formally edited.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Printed in Austria.

CONTENTS

ACKNOWLEDGEMENTS

This guide was produced by the United Nations Office on Drugs and Crime (UNODC). It was developed with generous funding from the Department of Foreign Affairs and Trade of Australia under the framework of the Asia-Pacific Joint Action Towards a Global Regime Against Corruption.

UNODC acknowledges with profound gratitude those who have contributed their expertise and experience to the development of this guide, and the experts who participated in the international expert group meeting held in Vienna on 28 and 29 June 2018:

Tomislav Ćurić, Regional Anti-Corruption Initiative, Bosnia and Herzegovina; Sandra Damijan, Faculty of Economics, Slovenia; Dimo Dimov, Ministry of Transport, Bulgaria; Davor Dubravica, Croatia; Lilian Ekeanyanwu, Technical Unit on Governance and Anti-Corruption Reform, Nigeria; Vladimir Georgiev, State Commission for Prevention of Corruption, North Macedonia; Tetiana Getmantseva, National Anti-Corruption Bureau, Ukraine; Silje Hanstad, Norwegian Agency for Development Cooperation, Norway; Wai-Chi Ho, Independent Commission against Corruption, China; Max Kaiser, Mexican Institute for Competitiveness, Mexico; Martina Koger, Federal Bureau of Anti-Corruption, Austria; Syafira Larasati, Corruption Eradication Commission, Indonesia; Gyula Pulay, State Audit Institution, Hungary; Lioubov Samokhina, Group of States Against Corruption, Council of Europe; Lise Stensrud, Norwegian Agency for Development Cooperation, Norway; Wahyu Dewantara Susilo, Corruption Eradication Commission, Indonesia; Erna Van der Merwe, Anti-Corruption Commission, Namibia; and Aslan Yusufov, Department for Monitoring the Implementation of Legislation on Combating Corruption, Russian Federation.

UNODC would especially like to thank the following experts who participated in the expert group meeting and provided direct feedback on the guide: Tom Caulfield, Procurement Integrity Consulting Services; Khalid Hamid, State Audit Institution, United Arab Emirates; Elizabeth Hart, World Wildlife Fund, United States of America; Richard Messick, Senior Contributor, Global Anticorruption Blog; and John Mugendi, Kenya Wildlife Service, Kenya.

UNODC wishes to acknowledge the contribution of Constantine Palicarsky of the Corruption and Economic Crime Branch, who was responsible for the development of the guide. The guide benefited from the valuable input of many UNODC staff members and consultants who reviewed and commented on various sections of this guide, including the following: Fernanda Barrera of the Liaison and Partnerships Office in Mexico, Francesco Checchi of the Regional Office for South-East Asia and the Pacific, Jenna Dawson-Faber of the Global Programme for Combating Wildlife and Forest Crime, and Giovanni Gallo, Tim Steele, Constanze Von Soehnen and Kari Rotkin of the Corruption and Economic Crime Branch.

ACRONYMS AND ABBREVIATIONS

COSO	Committee of Sponsoring Organizations of the Treadway Commission
DOI	Digital object identifier
ERM	Enterprise risk management
INTOSAI	International Organization of Supreme Audit Institutions
ISO	International Organization for Standardization
ISSN	International standard serial number
IT	Information technology
SDGs	Sustainable Development Goals
UNODC	United Nations Office on Drugs and Crime

INTRODUCTION

Notwithstanding the fact that the vast majority of public servants perform their duties honestly, all organizations and government institutions face the risk of corruption. Whether through the awarding of public contracts, collection of taxes or other revenues, payment of social benefits, or in any of the other ways in which a government interacts with its citizens, there is the ever-present chance that a public official will engage in corruption through the misuse of specific powers, insights and access to information. Likewise, persons interacting with government institutions and public officials might try to use corruption to, for example, influence or circumvent rules, procedures and decisions. The challenge most organizations face is identifying the points in their operations where corruption is most likely to occur, developing and implementing strategies to prevent this corruption from occurring in the future, and ensuring that all members of the organization work with integrity to achieve the organization's mandate.

Listing just a few examples, corruption risk management can contribute to the enhanced delivery of services to citizens that is neutral and objective, reduce loss of revenue, or safeguard law enforcement operations and human security. It is therefore of key importance for the rule of law and sustainable development.

By implementing corruption risk mitigation strategies, organizations can be better placed to meet their own objectives.

The United Nations Convention against Corruption requires States parties to have "effective and efficient systems of risk management and internal control" as a means for promoting "transparency and accountability in the management of public finances".[1]

Eliminating corruption is also essential for the achievement of the Sustainable Development Goals (SDGs) and the targets adopted by Member States on 25 September 2015, forming the 2030 Agenda for Sustainable Development, which represents a plan of action for people, planet and prosperity.[2] The Goals and targets are integrated and indivisible, and balance the economic, social and environmental dimensions of sustainable development. The interlinkages and integrated nature of the SDGs are of crucial importance in ensuring that the purpose of the 2030 Agenda for Sustainable Development is realized. This means that eliminating corruption, which is explicitly recognized in target 16.5, and developing effective, accountable and transparent institutions at all levels, as foreseen in target 16.6, are vital for the achievement of every SDG.[3]

UNDERTAKING A CORRUPTION RISK ASSESSMENT

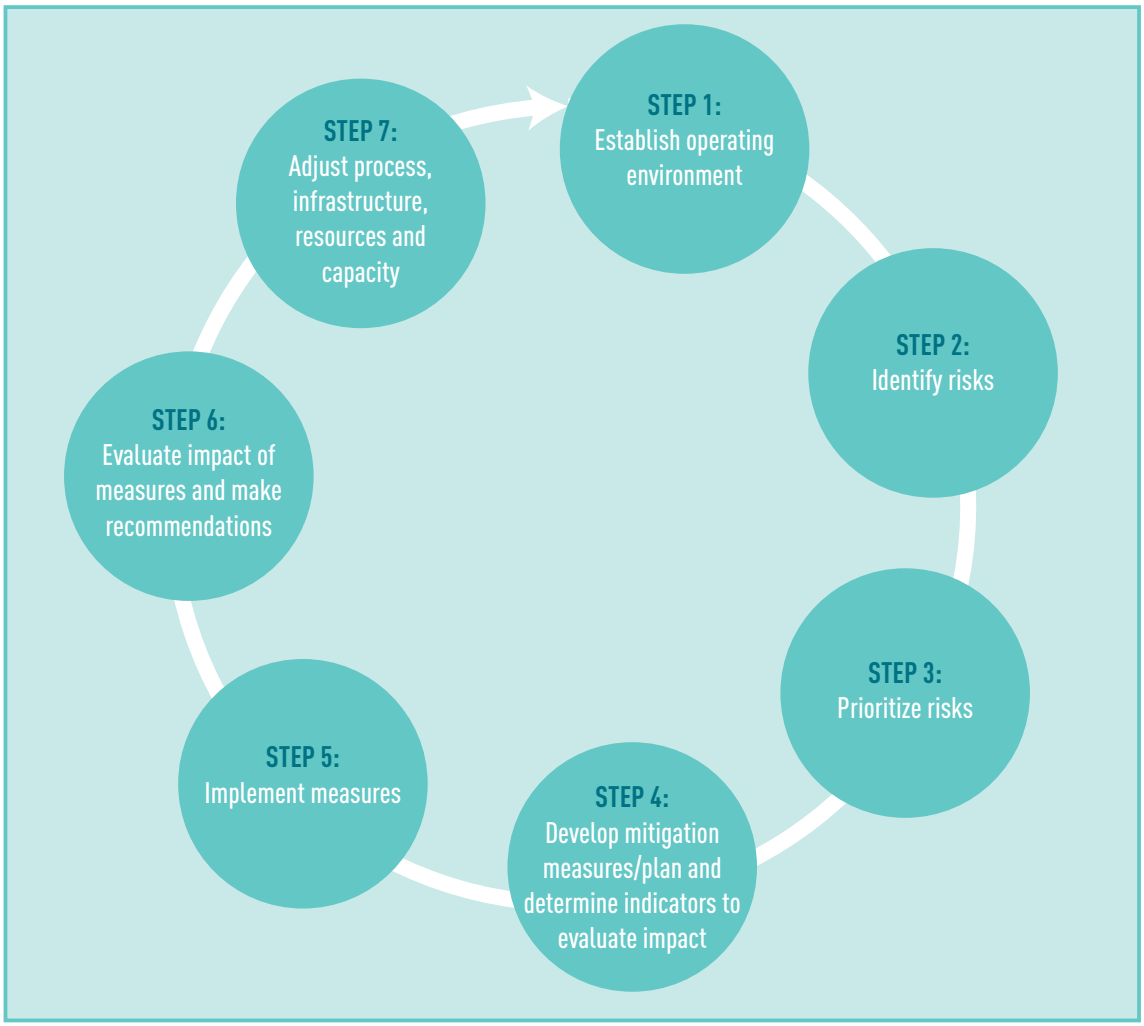
A corruption risk assessment is a systematic tool that can be used by public organizations to identify corruption vulnerabilities within their operations and devise efficient, cost-effective strategies to mitigate those vulnerabilities or risks. The goal of any risk assessment is to identify a realistic set of potential areas or scenarios that may be vulnerable to corruption, determine which should be prioritized, and develop and implement mitigation measures.

[1] United Nations Office on Drugs and Crime (UNODC), *United Nations Convention against Corruption* (2004), art. 9, para. 2*(d)*, p. 13.

[2] "Transforming our World: the 2030 Agenda for Sustainable Development" (General Assembly resolution 70/1), Sustainable Development Goals and targets.

[3] Target 16.5 aims to "substantially reduce corruption and bribery in all their forms".

Figure 1. Diagram of the risk assessment and mitigation plan process



Structure

The guide describes how to identify and treat specific corruption risks, and how to institutionalize structures within an organization to ensure that corruption risk mitigation becomes part of the organization's day-to-day activities.

The structured risk assessment suggested in this guide leads public organizations through a step-by-step process to establish the operating environment (context) in which the assessment will occur, identify the corruption risks to which they are exposed, evaluate which of these are the highest priority risks to tackle, and develop a plan to mitigate these highest-priority corruption risks efficiently with the limited resources available.

The guide begins by explaining the standards set forth in the United Nations Convention against Corruption. The next section focuses on preparing the risk assessment. This includes, first, establishing the scope of the risk assessment and whether the assessment should be comprehensive or target-specific. The organization would also have to decide if an internal or external assessment is the ideal choice, depending on its specific needs and composition. Finally, the appointment of a working group or similar team leading the exercises, as well as training and feedback mechanisms, is addressed.

The final section of this guide deals with the actual risk assessment. The appointed working group should undertake a structured step-by-step risk assessment and management process, with the first step being an

evaluation of the operating environment of the organization, including mandates, functions and stakeholders. Step two is for the working group to identify potential external corruption risks, while step three should be an analysis of those risks. The fourth step is an evaluation of the likelihood and impact of the identified corruption risks in order to prioritize the most pressing ones. Finally, the fifth step is the treatment of corruption risks through a mitigation plan which consists of reviewing the existing controls, determining the needs and feasibility of new controls, preparing a risk mitigation plan, and finally, delivering the risk mitigation plan. While every risk assessment is influenced and determined by an organization's culture and mission, the process articulated in this guide is a universal approach that can easily be adapted to every organization's needs.

Eradicating corruption within an organization is not a single event. Criminals will continuously attempt to find new ways to exploit public sector organizations and the public budget. These organizations must, if they are to remain effective, have processes in place to identify and counter these attempts. Once corruption risks are identified, prioritized and addressed, the next assessment cycle should begin to determine any outstanding risks, the effectiveness of the mitigation measures already implemented, and any new measures that should be introduced. Reiterating this process over time will strengthen an organization's ability to effectively minimize corruption risks and consequently prevent corruption schemes from occurring.

Purpose and audience

This guide aims to support public sector organizations, including integrity officers and other members of staff involved in integrity and anti-corruption efforts, to establish and institutionalize corruption risk management, as well as to empower anti-corruption authorities in undertaking their preventative functions. For the purposes of this guide, public sector organizations include any public institution, government body or agency, or national anti-corruption authority. Where an organization's resources are plentiful, a corruption risk mitigation plan might establish comprehensive operating procedures with clear audit trails, adequate levels of supervision and controls,[4] and clear written rules that guide officials on how to follow such procedures.[5]

This guide recognizes that many public organizations simply do not have the required human or financial resources or the knowledge to implement such comprehensive mitigation measures. Engaging in lengthy and often expensive risk identification exercises can lead organizations to spend their available resources on detecting risks, leaving few resources with which to implement the required mitigation measures.

The purpose of this guide is to support public organizations in effectively conducting risk assessments, within the margins of their available resources. To do so, this guide assists organizations in identifying the most efficient ways to implement realistic mitigation measures for the most harmful corruption risks, as identified by the organization.

The guide recommends an organization-led effort. Self-assessments are conducted more quickly and at less cost than assessments conducted by external parties. However, this guide recognizes that organizations may not feel confident undertaking a self-assessment or may not have the technical skills, or there may be legislation which stipulates the enrolment of a third party. In such cases, the organization should enlist the help of one or more external parties experienced in conducting corruption risk assessments.

The guide is informed by the experiences of the United Nations Office on Drugs and Crime (UNODC) in providing technical assistance to States parties to the United Nations Convention against Corruption and their public administrations. The process it recommends is outlined in figure 1 and is consistent with the International Standards Organization (ISO) ISO 31000 guidance for assessing and managing risks.[6]

[4] Internal controls are "the whole system of financial and other controls, including the organizational structure, methods, procedures and internal audit, established by management within its corporate goals, to assist in conducting the business of the audited entity in a regular economic, efficient and effective manner; ensuring adherence to management policies; safeguarding assets and resources; securing the accuracy and completeness of accounting records; and producing timely and reliable financial and management information". See *ISSAI 1003 Glossary of Terms to the INTOSAI Financial Audit Guidelines*, p. 57; see also *IFAC Glossary of Terms* (February 2009), www.ifac.org/system/files/downloads/a005-2010-iaasb-handbook-handbook-glossary.pdf

[5] The enterprise risk management methodology of the Committee of Sponsoring Organizations of the Treadway Commission has, over time, become the international standard for effective risk management best practice, and forms the foundation for International Standards Organization (ISO) standards such as *ISO 31000: Risk Management: Principles and Guidelines* (for more details, see annex 2).

[6] ISO, *ISO 31000 Risk Management Process, ISO 31000:2018.* Available at: www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

Chapter 1.

DEFINING CORRUPTION AND CORRUPTION RISK

The United Nations Convention against Corruption recognizes that there is no single, agreed definition of corruption and acknowledges that it is a continuously evolving phenomenon that is affected by various factors. Legal frameworks can thus differ in their descriptions of corruption. Considering this, the Convention offers a list of universally agreed manifestations of corruption, leaving each State free to go beyond the measures set forth in the Convention. These measures are:

- *Active bribery.* The promise, offering or giving to a national public official, foreign public official and official of public international organizations of an undue advantage, in order to act or refrain from acting in matters relevant to official duties
- *Passive bribery.* The solicitation or acceptance by a national public official, foreign public official and official of public international organizations of an undue advantage, in order to act or refrain from acting in matters relevant to official duties
- *Embezzlement.* Theft or misappropriation of property, funds, securities or any other item of value entrusted to a public official in his or her official capacity
- *Bribery in the private sector.* Active or passive bribery by any person who directs or works, directly or indirectly, in any capacity, for a private sector entity
- *Embezzlement of property in the private sector.* Embezzlement by any person who directs or works, directly or indirectly, in any capacity, for a private sector entity
- *Abuse of functions.* Performance of, or failure to perform, an act in violation of the law by a public official in order to obtain an undue advantage
- *Trading in influence.* Abuse of a public official's influence with an administration, public authority or State authority in order to gain an advantage
- *Illicit enrichment.* A significant increase in assets of a public official that cannot reasonably be explained as being the result of his or her lawful income
- *Money-laundering.* The concealment of the origins of corruptly obtained money, often by means of transfers involving foreign banks or legitimate businesses
- *Concealment.* Hiding or continued retention of property that has resulted from corruption

A distinction should be made between what constitutes "corruption" and what constitutes a "corruption risk". While corruption refers to an offence that has already occurred, a corruption risk is the potential for an offence of corruption to occur. In this sense, responding to corruption is reactive, whereas responding to an identified corruption risk is proactive. It must be stressed that this guide focuses purely on future corruption risks.

Chapter 2.

PREPARING FOR THE RISK ASSESSMENT

2.1 ESTABLISHING THE SCOPE OF THE RISK ASSESSMENT

The process shown in figure 1, like any other tool, will only be effective if implemented with the genuine desire to detect and fix any real shortcomings identified within the organization. It is most suitable for environments where the management of the organization is convinced of the need to better manage corruption risks, and it will only be successful where the organization's leadership and staff are genuinely invested in the process. Securing the commitment of the organization's management and employees is essential. The scope and process of a risk assessment and its potential outcomes should be discussed with senior management as a first step.

In preparing for a risk assessment, the organization should decide if the process will be comprehensive or target-specific. Many private sector organizations identify every potential corruption risk to demonstrate the adequacy of their compliance strategies. This comprehensive process may not be necessary for all public sector organizations. This guide is written primarily for organizations aiming to focus on identifying and addressing targeted, specific corruption risks.

The motivation for engaging in a corruption risk assessment process may vary. A corruption scandal, an audit finding, a media report, or the adoption of a national anti-corruption strategy requiring all public organizations to conduct a corruption risk assessment and devise a prevention plan are all possible motivators for conducting a risk assessment. Organizations may also wish to proactively assess their vulnerabilities to prevent future risks.

A focus on the immediate problems faced by an organization can be a useful starting point when these concerns become apparent. Multiple scandals, a decline in cash receipts, a rise in citizen complaints or an inexplicable change in an employee's standard of living can all serve as agents for the assessment process. In addition, focusing on visible, identifiable problems can help manage an unfortunate side effect of some anti-corruption efforts, which is the risk of a witch-hunt developing within the ranks of the organization. It is easier to build a consensus among the organization's personnel on the need to address performance problems, rather than on a general sense of fear built around the danger of corruption.

Whatever the motivation for implementing a corruption risk assessment process, there is likely to be hesitation about, and in many cases outright resistance to, the process, especially during the initial stages. UNODC has observed some of the reasons for such resistance (listed in box 1).

Box 1. Reasons for resisting the initiation of a corruption risk assessment process

- Staff fear that a focus on corruption will lead to an effort to find a scapegoat or might result in a campaign against employees in a certain unit or location.
- Stakeholders are concerned that addressing corruption will disrupt an organization's operations for an extended time.
- Stakeholders worry that corruption concerns will lead to radical, unexpected changes in an organization's operations and may upset established ways of interacting with the organization.
- Management may fear corruption concerns are a way to discredit and replace their positions.
- Management may fear that the reputation of the organization will be damaged, as others may see a corruption risk assessment as an admission that their organization is "rotten".

2.2 INITIATION OF THE RISK ASSESSMENT PROCESS

Any activity requires resources, and corruption risk assessments are no exception. The key resources required are experienced staff and funds to secure outside support if needed (facilitators, auditors, forensic accountants, fraud examiners, etc.). Management should also support staff by redistributing workloads or temporarily reassigning projects to ensure that team members have the necessary time to focus on conducting the risk assessment.

Organizational processes must have an owner. Deciding who will own the risk assessment process (and who will be responsible for its effective completion) is a critical first step. The ownership of the corruption risk assessment is usually vested in a specially appointed group – the corruption risk assessment working group or task team. However, the composition of the team and its position in the hierarchy of the organization depends on several factors outlined below.

Activities at the assessment stage should be carried out by a working group of organizational staff members appointed by management to conduct the assessment and develop a mitigation plan. The staff involved at this stage should be explicitly directed to perform these functions. If not, there is a danger that their immediate supervisors will not release them from their regular duties, treating their time conducting the assessment and mitigation plan as an extra burden to be worked into their schedule only if time permits.

Larger organizations will require a larger working group and need more time to assess risks and develop a plan. A good rule of thumb is that several brainstorming sessions followed by two to three months of data collection, debriefing and validation meetings is the minimum requirement. Box 2 lists the items that should be considered in a realistic budget.

Box 2. Required resources

- *Staff time.* The amount of time staff members must spend on the assessment and the level of expertise needed to perform the required tasks.
- *Outside adviser(s).* This includes costs for travel and fees, which may be paid by the organization or by external sources (auditors, forensic accountants, fraud examiners, consultants).
- *Travel.* This will depend upon whether the organization's offices are spread out across the country or in one location or a single city.
- *Communications.* This includes costs for Internet service, postage, telephone calls, etc.
- *Printing and duplication.* This includes costs to cover the preparation of data collection instruments, reports and other documents.
- *Supplies and equipment.* This covers the costs of any required supplies and equipment (e.g. computers, packaged software) that must be purchased or rented for the assessment.

Source: Organisation for Economic Co-operation and Development, *Public Sector Integrity: A Framework for Assessment* (2005).

Factors affecting the composition of the working group

- *The size of the organization.* Large, complex organizations have different requirements than smaller, agile ones. A simple rule would be that the greater the need for coordination, the higher the positions of the team members should be.
- *The mandate and operational structure of the organization.* More complex structures with a range of mandates require an assessment approach which incorporates staff from multiple departments and divisions. Conversely, smaller organizations with a single, well-defined mandate may assign the corruption risk assessment to a small team of officials. Very small organizations might even have one or more working group members seconded from a larger organization.
- *The cooperative or adversarial nature of the organization's relationship with stakeholders.* The nature of these relationships must be considered when determining whether the working group should have any members drawn from stakeholder organizations, the public at large or non-governmental organizations. The involvement of these stakeholders and the extent of such involvement will depend on the link between them and the organization. For example, a customs organization will have a close and ongoing relationship with importing firms and their business associations (and so representatives from these firms could be considered for inclusion in the working group, where appropriate) whereas a tax organization will have less of a link to taxpayers.

There is no one-size-fits-all approach when establishing a well-functioning working group. The composition of the group will need to be tailored to the individual organization; however, based on UNODC experience (and bearing in mind that the goal of the working group is to identify corruption risks and to suggest mitigation measures), it is logical that, at a minimum, the members of the team should have extensive experience working in all operational areas and support services within the organization.

Skills required in the working group

Typically, the composition of a working group would include members with the following: a thorough understanding of how the organization functions; backgrounds in law, internal auditing, internal controls, human resources, and/or procurement; experience in performing risk assessments; and knowledge of the key organizational mandates. Depending on the number of organizational mandates (and their complexity), one or more officials with knowledge of the organization's operations should be involved.

Many internal auditors perform "risk assessments" in the context of their assigned projects. It is important to understand that an organizational or division-level corruption risk assessment as described here is different from an audit risk assessment. An internal auditor performing an audit risk assessment uses a risk-based approach to determine which of a company's processes and procedures to assess and then performs tests to determine the adequacy and extent of staff compliance with such procedures. Not all procedures are assessed in every audit cycle. An organizational or division-level risk assessment is much broader. It calls on the management of an organization to take a comprehensive look at the entirety of the organization's operations to determine where and to what extent corruption risks are likely to exist. Rather than to provide comfort as to the level of compliance with such systems, an organizational or division-level assessment is done for the purpose of addressing identified corruption risks. Such an assessment may show that internal policies and procedures are insufficient for this purpose, even if staff consistently comply with them.

Thus, by selecting the correct personnel, the working group will acquire the necessary hands-on experience and knowledge of the organization's various operations. It will also serve as a two-way communication channel, ensuring that the working group can gather information from all parts of the organization, and that the various parts of the organization are in turn informed of the work of the group.

The working group should be headed by a senior and knowledgeable official who can secure the active participation of group members, and who can lead the process without requiring constant, direct access to the leadership of the organization. Additionally, where personnel are spread out geographically, it is critical to include officials from the field in the working group.

Communicating the establishment of the working group

Experience shows that organizational personnel can occasionally misunderstand the process and confuse the risk assessment phase with an investigation. Some may even fear that their unit or their job may be in jeopardy. The best way to manage such fears is through clear, regular communication to employees about the process and its intended outcome, and by ensuring free and open discussion between the working group members and other staff.

A directive establishing the team, naming its members, and briefly explaining the process should be issued at the outset by the leadership of the organization. The directive should be informative, emphasizing that the process is not investigatory. It should also outline the rules governing record-keeping, document storage, and other administrative matters. The directive should clearly communicate to all organizational staff the importance of cooperating with the working group.

Where external stakeholders are to be consulted, the directive should name those groups that will participate in the process. If decisions on who from outside the organization will be involved in the process have yet to be made, the directive should note that this information will be provided later in the same format.

Risks of including external stakeholders in the working group

It may be reasonable to open the process to external scrutiny, or to include stakeholders from outside the organization in the working group, such as representatives from private sector entities who work closely with the organization and possess relevant information. However, careful consideration should be given to the risks associated with such a decision. These risks include sharing sensitive information with outsiders (which the working group may not have the authority to do) and information leaks (which may see the entire exercise fall hostage to political power struggles), as well as the practical risk of discussions losing their focus or decisions being delayed unnecessarily. These factors (and others relevant to the organization) should be carefully balanced when a decision is made on whether to include external stakeholders in the working group.

2.3 THE ROLE OF ORGANIZATIONAL PERSONNEL

Benefits of self-assessment

No one should know an organization's procedures and vulnerabilities better than those who work for it. A process led by staff from the organization is the preferred course of action because it forces the organization to identify and confront its own vulnerabilities, as well as the corruption risks those vulnerabilities create.

Staff can tailor the assessment methodology to exactly what is needed and will know what information and data are available or can be easily and cheaply gathered. A self-assessment will also help to build or strengthen a culture of integrity within the organization.

Furthermore, it has been observed that when an internal working group conducts the assessment and develops the mitigation plan, the likelihood that the rest of the organization's staff will accept and implement the results increases. A self-assessment is much more likely to smoothly integrate with the organization's operations and produce corruption mitigation measures that are relevant and actionable.

Potential drawbacks of self-assessment

However, even with willing leadership and a robust working group, self-assessment has its drawbacks. For example:

- Staff may be reluctant to objectively and frankly identify the types of corruption to which the organization might fall victim. Fears may arise from concerns such as retaliation from colleagues or management, or the potential damage to the reputation of the organization. This reluctance can result in the working group's failure to identify some forms of corruption to which the organization is very vulnerable, or, if they are identified, in its failure to prioritize them.
- It is likely that the majority of staff within an organization will not have been specifically trained to identify many common forms of corruption. For example, a form of corruption related to procurement is the tailoring of tender specifications to favour a particular supplier. Staff may observe that a particular supplier is always used, or they may notice an unusually high price being paid for a low-cost service, but having not been trained appropriately, may not be able to identify these as potential warning signs of corruption. If there is no one available within the organization to describe with authority how corruption schemes may occur, then external facilitation may be required. Note, however, that the tailoring of tender specifications may not be a result of corruption if only one supplier can meet the organization's needs and it is possible to obtain an exception to the normal competitive procurement process. In this case, the risk assessment can serve to educate staff on how and in what circumstances such exceptions can be sought.

2.4 THE ROLE AND COMPOSITION OF EXTERNAL FACILITATORS

The risks associated with a self-assessment can be remedied by recruiting one or more individuals who are not affiliated with the organization to assist the working group. The role of external advisers is to facilitate the risk identification exercise rather than participate in the working group. However, achieving this goal is a delicate balancing act.

The facilitators should not tell the working group what they feel the problem is, or where the corruption risks lie. They must be extremely careful not to suggest corruption schemes that they feel may pose a risk to the organization (and therefore unnecessarily narrow the scope of any risk identification conversations within the working group), while at the same time, they must provide enough information on how to identify corruption risks to empower participants to understand the risks to which their organization may be exposed.

Who is chosen as the facilitator(s) depends on the requirements of the organization and the motivating factors for the assessment. That being said, in all circumstances the facilitator(s) will require a strong understanding of the sector and environment in which the organization operates. An organization with little experience in corruption prevention should consider someone with the ability to describe what corruption may look like in a range of common situations and with the skills and experience to work with the organization throughout the process until a corruption risk mitigation plan is implemented.

It may also be the case that the assessment is driven by problems arising from poor internal controls. If so, an auditor, accountant or other individual familiar with the recommendations of the Committee of Sponsoring Organizations of the Treadwell Commission (COSO) and the International Organization of Supreme Audit Institutions (INTOSAI) might be desirable.[7]

The professional affiliation of the external adviser(s) hired to facilitate the risk assessment must also be considered. Would organizational personnel feel comfortable working with someone from a supreme audit institution, or an ethics committee, or an anti-corruption agency? The affiliation of an adviser can create a reluctance among the working group to share sensitive information, for fear it could later be used against

[7] See annex 1 for more details on the Committee of Sponsoring Organizations of the Treadwell Commission (COSO) and the International Organization of Supreme Audit Institutions (INTOSAI).

them. Such affiliations should obviously not immediately disqualify an external adviser; however, the issue of affiliations should be carefully considered.

One alternative is to use an international adviser as the facilitator, unattached to any local or national organization but with expert knowledge in the relevant substantive areas. UNODC has observed that such international advisers often combine expertise with a sense of distance that makes organizational staff more willing to speak candidly. However, language differences, cultural issues and lack of expertise on specific national laws and procedures may reduce the suitability of an international consultant.

2.5 EMPOWERING THE WORKING GROUP

Once the working group has been assembled, its members will need to be empowered to perform their functions. It is recommended that an internal expert or external facilitator conduct an initial briefing session on risk management, the risk assessment and why their organization is conducting one, and their roles within the process.

As a starting point, the facilitator should assess what the participants understand corruption to be and explain to them that the purpose of the corruption risk mitigation plan is to enhance current integrity controls or design new ones. Doing so will identify vulnerabilities and reduce the chance that individuals within or external to the organization might engage in actions that harm the organization, either financially, operationally or reputationally.

For this initial briefing session, a one-day workshop will ordinarily suffice. However, it is recommended that, during the session, the leadership of the organization is present and states clearly the importance of the process, the background that led to the launch of the assessment, and that it has the full support of the most senior levels of leadership within the organization.

In addition to empowering the working group to identify corruption risks, the workshop should also be used to agree on administrative and technical matters. These may include but are not limited to the organization and duration of the process, the tasks of the individual members of the team, certain procedures on how to organize brainstorming sessions, and how to collect and process information. Everyone involved in the working group must understand that this process is not to identify individuals who may have committed or may currently be engaging in corruption or fraud. The working group should agree on how to handle such information if it is accidentally discovered, such as referring it to management for further investigation.

Organization leaders, along with those running the workshop, must be careful not to influence the assessment by saying what they think the key issues are, or by citing common corruption risks to which they think the working group should be alert. In the early stages of the process, working group members will be looking for signals of what is expected of them and how far they can go. Innocuous mention of specific corruption risks that workshop leaders feel merit attention can lead working group members to believe these, and only these, are what they should be looking for or are tasked to "uncover". Leaders may, however, choose to share a list of common corruption risks for the benefit of the group without commenting on their likelihood or relevance.

One way to open the discussion is with a broad overview of the ways in which corruption can strike any public organization. Table 1 summarizes the types of corruption risks to which all public organizations are susceptible, dividing them into vulnerabilities that arise from outside the organization and those that arise from within. Treating some vulnerabilities as a result of external actors can itself be helpful in starting a discussion, tempering any implication that the exercise is specifically targeted at individuals or units within the organization. As group members become more comfortable with candidly acknowledging risks from external sources, those that arise internally can be introduced into the conversation.

It will also be important to ensure that working group members limit their discussion to genuine forms of corruption. In some countries, the term "corruption" is used loosely to denote any conduct that deviates from responsible governance. UNODC experience shows that the use of such a definition is often a precursor to an unfocused assessment and is likely to result in a mitigation plan that contains few, if any, concrete actions.

In the initial briefing, therefore, it should be stressed that the purpose of the assessment is to determine how and where the organization's ability to operate might be compromised by offences listed in chapter III of the United Nations Convention against Corruption (see chapter 1), or by any other acts defined as corruption in national legislation. More general organizational inefficiencies and performance problems should be included in the assessment only where they create a clear risk of corrupt activities.

Table 1. General corruption vulnerabilities in public sector organizations[a]

	REASONS FOR CONTACT	EXAMPLES OF VULNERABILITIES
EXTERNAL Relations with the private sector or the public Undue influence, personal favouritism or bribery affect decisions	Collect money	Exemption/undercollection of taxes, licence fees, import duties, assessments
	Issue contract/order	Favouring one supplier in preparation of tender or contract award, unnecessary change orders
	Pay out money or benefit	Benefit conditioned on kickback or favour, overpayment
	Issue permit/licence/ approval	Passports, building permits and inspections, drivers' licences
	Enforce law or rule	Violation not reported or false report threatened, investigation or prosecution dropped
	TYPE OF ASSET	**EXAMPLES OF VULNERABILITIES**
INTERNAL Management of public assets Embezzlement, fraud, loss due to corruption	Money	Receipt of licences and admission funds, expense reimbursement, salary/overtime
	Equipment	Organization equipment or stockpiles
	Information	Theft/sale of confidential information regarding the tender or the organization's future acquisitions, national security data

[a]Benner and de Haan, Netherlands Court of Audit, *SAINT: A Tool to Assess the Integrity of Public Sector Organizations.*

2.6 CREATING FEEDBACK MECHANISMS

As explained in annex 3, a formal, thorough risk assessment provides for continuous feedback through regular communication and consultation with relevant stakeholders. However, as noted above in the discussion on the working group's composition, too great an involvement with those outside the organization can have its own drawbacks. Insiders may be less candid about the risks the organization faces, and leaks of preliminary findings and conclusions can politicize the effort, or see the process descend into a search for a scapegoat.

However, keeping stakeholders informed and seeking their thoughts as the process moves forward can be extremely valuable. They can help build support for the actions contained in the mitigation plan and can bring their own experience and insight to the table, providing additional information on corruption risks and what can be done to mitigate them. One solution is to provide, either to the public generally or to a select group of stakeholders, periodic briefings on the progress of the risk assessment. Other solutions include the establishment of an advisory panel of stakeholders or formal or informal surveys of stakeholders.

Again, the decision on when and how to involve stakeholders will be determined by the precise conditions at play, along with the organization leaders' judgment of how best to reap the benefits of external stakeholder participation while minimizing any detrimental effects.

Chapter 3.

THE RISK ASSESSMENT AND MANAGEMENT PROCESS

The goal of the risk assessment and management process is to produce a set of actions that the organization can take to prevent and detect indications of corruption.

3.1 STEP 1 – EVALUATING THE OPERATING ENVIRONMENT

The first step is for the working group to reflect on the external factors that shape the organization's behaviour, the behaviour of its employees, the powers the organization has over these factors and what constraints it faces in exercising them (see box 3). For example, it may be that procurement is an area where an organization's risk of corruption is high, but its power to change procurement procedures may be limited by public procurement laws, or suppliers may be able to block changes by appealing to sympathetic parliamentarians or by challenging the organization's actions in court.

In examining the external context, the working group should consider a broad range of factors that affect the organization, including the legal, regulatory, financial, technological, economic, natural and competitive environment.[8] Applied to a public organization, the most important external factors are likely to be legal and political. What are the laws governing the operations of the organization? What powers do these laws grant the organization? Who oversees the organization? Parliament, the supreme audit institution, the courts or another body? How does their oversight affect operations?

The working group might also consult an internal auditor or inspector, or an external law enforcement or anti-corruption authority, about corruption cases or complaints involving the organization's operations. Depending on the context, other sources to query could include the organization's stakeholders, civil society groups or the media. Regardless of whom the working group determines would be a useful source of information, a sample set of questions to pose is provided in box 3.

[8] Robert B. Pojasek, *Organizational Risk Management and Sustainability: A Practical Step-by-Step Guide* (Taylor & Francis Press, 2017).

Box 3. Assessing how external factors affect an organization's corruption mitigation plan

- What are the laws governing the organization's operations and what powers do they grant to the organization?
- What government bodies oversee the organization? The parliament, a supreme audit institution, the courts?
- How do these bodies react to reports of corruption?
- Who investigates corruption allegations? An internal inspector, the police or an anti-corruption body?
- Who are the organization's stakeholders?
- Are the stakeholder's interests aligned with those of the organization?
- Which civil society groups monitor its behaviour?
- How much media coverage does the organization receive?
- To what extent are formal rules and institutions adhered to?
- Do informal institutions influence the organization's operations or the behaviour of its stakeholders?

Internally, the organization must consider the context surrounding its governance, organizational structure, roles and responsibilities, as well as specific procedures such as those involving procurement processes and personnel management.

Key issues to consider in virtually every assessment are the laws and regulations governing the recruitment, promotion, discharge and conduct of public servants, as well as the integrity and anti-corruption laws that cover conflicts of interest. Are employees required to disclose their financial interests? Does the organization have an ethics code? Are there channels for reporting possible corruption, and do protections exist for those whistle-blowers? What rules govern the management of public finances and internal and external audits?

Box 4. Factors that comprise an organization's internal control environment

1. Personal and professional integrity of personnel, including support for internal controls
2. Commitment to competence
3. Management's philosophy and style (tone at the top)
4. Organizational structure
5. Human resource policies and procedures

Source: INTOSAI, *INTOSAI GOV 9100: Guidelines for Internal Control Standards for the Public Sector*.

The current INTOSAI internal control guidelines for public sector organizations identify five factors that make up the foundation of any organization's internal control environment. Listed in box 4, the guidelines highlight how these five factors provide the discipline and structure, as well as the climate, that influences the overall quality of internal control.[9] Weaknesses in any of them or lapses in their application put the organization at significant risk that some form of fraud or corruption will occur.

[9] INTOSAI, *INTOSAI GOV 9100: Guidelines for Internal Control Standards for the Public Sector*.

A major advantage of a self-assessment is that those conducting it are likely to know the organizational context well, and little time will be required to review it. Particularly where the intention is to implement a modest first attempt at assessing a manageable set of problems, this step can be addressed quickly.

Nonetheless, at least one meeting of working group members should be devoted to discussing the organizational context, using the questions in box 3 to steer the conversation. Some group members may, for instance, not have a complete picture; others may be misinformed about some details. The working group leader should ensure that all group members have a common, accurate understanding of the environment in which the organization operates, and what powers it has available to affect that environment. A memo summarizing this information is an effective way to ensure this is the case.

3.2 STEP 2 – IDENTIFYING POTENTIAL CORRUPTION RISKS

The second step of the process is to identify the types of corruption risks to which the organization is, or may be, exposed. During this step, the working group will examine the functions an organization performs and identify where a dishonest actor could potentially profit from illicit actions.

Group members will draw on what they know about their organization's operations. It will often be useful to supplement their knowledge and confirm it through interviews with colleagues, focus groups and reviews of documentation.

It is recommended that the process of identifying corruption risks take the form of a brainstorming session, where the working group members freely exchange ideas to compile a list of corruption schemes to which the organization is potentially vulnerable. One way to do this is to ask the working group to "think like a thief"; that is, like someone wishing to gain an advantage by evading procedures or legal requirements.

Where the starting point is a more generalized pre-emptive concern about possible corruption, it is important to emphasize to group members and organizational staff that this is a "what might be" or "what if" exercise, not an investigation. An experienced outside adviser can be particularly helpful here, raising experiences reported in similar organizations in other countries and asking if something like this "is possible" or "might occur" within the organization in question. Employee surveys can also be useful, especially if employees have confidence in the anonymity of their responses.

During the brainstorming session, one way to initiate the identification process is to ask the working group to identify specific corruption risks and scenarios which they feel could strike the organization in the future. A very good predictor of what may happen in the future is what is already known to be happening. Where the corruption scenarios being described are taking place within the organization, the working group needs to decide how to segregate the corruption risk mitigation exercise from any enforcement processes.

Identification of vulnerabilities and corruption risks at an organizational level can be done in a number of ways, including the following:

- *Identifying underperforming areas of the organization*. Examples could be departments in which less money is being collected than would be expected given historical trends, or a unit in which fewer licences, permits or other services are being provided than normal. Procurement issues would include areas where the quality of the goods, services or construction work delivered is unreasonably low, or the price unreasonably high. Complaints of, or perceptions of, nepotism or abuse of office might also provide an indication as to where to focus.
- *A review of example corruption scenarios* can, if treated with extreme caution, be carried out, as they can prompt discussions in addition (or as an alternative) to a brainstorming session. Annexes 5–14 of this guide contain examples that may help. Annex 5 describes the different ways that bribes negatively affect public employees, annex 6 describes various embezzlement schemes UNODC and partner Governments have uncovered, annex 7 describes the methods used to cheat on expense reimbursements, and so forth.

If group members find it difficult to start a discussion about corruption during their initial meetings, the leader or facilitator of the group must find ways of encouraging the discussion without influencing its direction. One way of doing this is by giving examples of common corruption risks and schemes while simultaneously emphasizing that these are not schemes to which the facilitator thinks the organization is necessarily exposed.

Box 5 provides six common ways public monies and assets can be stolen; these can be shared during the brainstorming session to encourage discussion. If the group happens to identify any of these schemes as posing a risk to the organization being analysed, the facilitator should ask a set of questions to determine whether the risk is genuinely relevant to the organization. The corruption scenarios and schemes described in annexes 5–14 provide additional "conversation starters" or "ice breakers".

Box 5. Some common forms of asset fraud and corruption

1. *Skimming.* Cash is diverted from the organization prior to it being recorded. For example, an organization employee collecting the admission fee to a park pockets some of the money.
2. *Larceny.* Cash is taken after it is recorded. More complex than skimming, it can involve recording the receipt in a different account and creating a false entry to hide the theft. When responsibility for receiving and recording the funds is divided between two individuals, at least two people must be involved.
3. *Fraudulent disbursements.* Money is paid for goods not delivered or services not performed. An employee hires a friend to spray for insects on weekends. The friend never does but submits a bill for services performed.
4. *Payroll.* Individuals appear on the payroll who never come to work or may not even exist. Employees claim for overtime not worked.
5. *Travel and per diems.* Employees claim expenses for trips not taken or overbill for a trip. Hotel employees in some countries regularly provide false or inflated invoices for a fee.
6. *Inventory theft.* Office supplies, furniture and other items that can easily be sold are not properly reported when the organization receives them or records are falsified after delivery.

Source: Singh and Bussen, *Compliance Management: A How-to Guide* (2015).

If the group members are chosen well, they will know the organization's recent experiences with corruption and, as a result, the amount of time needed to find and review old records can be minimized. There can often be an excessive emphasis on gathering and analysing information regarding the organization's past experiences with corruption, examining in detail every report and every allegation of possible wrongdoing. This can divert attention from the identification and treatment of major corruption risks that have not yet materialized.

Too much effort can also be invested in listing the hundreds of specific ways in which corruption might affect the organization. The purpose of step two of this process is not to list every form of corruption risk to which the organization may theoretically fall victim, but instead to produce a realistic, manageable list of risks from which priorities can then be determined.

How long the list should be will depend first on how many functions the organization performs. For instance, the list of potential corruption risks for an organization that collects business registration fees, issues operating permits, and procures goods and services will be longer than the list for an organization that only issues permits. As the working group compiles the list, it should look for ways to consolidate individual vulnerabilities into broader categories. Employees at various locations may be responsible for accepting cash payments from the public for different services. Rather than listing each location and the money collected

for each service as a separate vulnerability, all of them could, for example, be listed under the heading "Chance of skimming cash receipts".

An experienced external adviser can be useful in several ways at this step. He or she can, as noted above, defuse any suggestion that, in developing a list, the working group members are suggesting their colleagues are corrupt. The adviser can also use his or her expertise to suggest how specific examples of corrupt acts can be grouped into broader categories to keep the list at a manageable size. Finally, he or she can keep the list relevant to the organization, reminding the working group to maintain focus only on the types of corruption that have a realistic chance of occurring within the usual operations of their organization.

Throughout the process, care should be taken to ensure that the adviser remains in the background. He or she could potentially introduce preconceived notions based on his or her experience with similar organizations in other countries, or endorse a "standard risk mentality" derived from previous work. The adviser's role is to facilitate discussions, not drive them. However, when the external adviser is an older, experienced anti-corruption specialist, and the working group members are younger and have less experience in corruption issues, the adviser can easily drive the process if adequate care is not taken.

Pitfalls to avoid

When developing the list of corruption risks, some common pitfalls to avoid include:

- *The safeguard illusion.* There is often an assumption that when adequate safeguards are in place to to protect against a risk, then that risk should be left off the list. However, most corruption schemes take place when people disregard the existing procedures and break the existing rules. Therefore, the mere fact that a procedure is in place does not guarantee protection against the corruption schemes that it is designed to combat or mitigate.
- *"Groupthink" and "elder dominance".* During working group sessions, "groupthink" can take hold. A desire for harmony or consensus can lead participants to minimize conflict and reach a consensus without critically evaluating differing opinions. Furthermore, in some environments, respect for authority may make younger or more junior participants reluctant to challenge the opinions of more senior members. The discussion leader may even, consciously or unconsciously, contribute to the problem by cutting off the discussion prematurely, or by appearing to stress the need for a consensus view.
- "Groupthink" or "elder dominance" can be avoided by being mindful of the problem when selecting participants for the group discussion. Another alternative is to form two groups, one with younger members and a second with more senior ones, although care should be taken to ensure that elder dominance does not occur once the two groups recombine. If these tactics prove unsuccessful, group members' opinions could be sought in advance or anonymously during the session and be presented for discussion without identifying their source.

At this stage in the process, it is better to include risks than to leave them out. The opportunity to exclude risks will come at the analysis and evaluation stages. This inclusive process should help overcome some of the potential biases discussed above.

3.3 STEP 3 – ANALYSING CORRUPTION RISKS

Once the working group has identified a list of potential risks, analysis can be undertaken to establish the nature and drivers of those risks. During this step, the working group could, for instance, interview staff, examine internal documents or review existing corruption controls. Internal documents may include past audit reports or investigations, or accounting or procurement records.

- *Interviews with organizational staff,* such as accountants, procurement officers and internal auditors can be carried out, either to identify issues or to confirm through analysis the findings from brainstorming sessions.

- *A review of internal documentation,* including complaints, disciplinary procedures and past cases, audit reorganization findings and the results of past investigations can be carried out. This can be a way to identify vulnerabilities and further analyse risks that have already been identified. This can also include a review of procurement and accounting records to identify unusual patterns (see box 7).
- *A review of current corruption controls* is a starting point suggested by some guides. Are they effective? Is there evidence they have failed to prevent the types of corruption for which they are designed? In any review of internal controls, an area to pay special attention to is whether management frequently overrides existing corruption controls. For example, is the need for a second signature on payment orders often waived? Is the rule requiring a person different from the one signing the warehouse receipt to issue a cheque overlooked? Such deviations can be evidence either of a breakdown in their effectiveness or an indication that they too often conflict with the performance of the organization's mission. Either finding is a strong sign that controls need to be re-examined.

This phase is designed to build an understanding of the nature of each identified risk. It is important to note that not all corruption risks are primarily financial in nature. In addition to financial risks, it is useful to think of the reputational risk associated with potential corruption, as well as the risk that corruption may hinder the ability of the organization to carry out its mandate. Categorizing the risk in this way will be particularly useful when thinking about its impact.

Consider, for example, an organization whose mandate focuses on ensuring that food products meet certain hygiene standards to maintain public health. A relatively small bribe could potentially lead to an inspector turning a blind eye, thereby allowing an infected product to reach the public, causing an outbreak of a potentially devastating disease. The financial impact of this on the organization may be negligible; however, the impact on the organization's reputation and ability to meet its mandate could be huge.

At this stage there should be a discussion as to why the risk is deemed to exist. Where the information is readily available, a review of relevant records to identify any unusual patterns that might be caused by corruption may be beneficial. If such information is not readily available, the mitigation plan should include provisions to ensure its future availability.

For example, using data to spot suspicious patterns in procurement awards can provide important indicators of possible corruption and fraud in the awarding of public contracts. Data on which firms win what percentage of public contracts, who the awarding organizations are, who is being paid what and when, and similar information can be easily collected, using e-procurement tools and payment data to identify areas where corruption is likely to occur.

3.4 STEP 4 – EVALUATING CORRUPTION RISKS

Identifying and addressing every conceivable corruption risk an organization faces, from an employee's one-time falsification of an invoice to an elaborate bribery scheme involving many employees and outsiders over time, is very likely to be impractical and unwieldy but may be necessary if the purpose is to demonstrate an adequate compliance regime. However, if the objective is to actually identify and address risks, a plan can only hope to address an excessively long list of possibilities if the organization has close to unlimited resources, which most do not. Any plan should therefore be realistic in prioritizing the corruption risks to which the organization is exposed.

During step four of the risk assessment process corruption risks are prioritized. The working group members should evaluate which corruption risks will be the priority to address in the mitigation plan. If the number of listed risks is small, and the resources required to address each risk is modest, prioritization may not be necessary.

Box 6. Subjective estimates of future risks

"[U]se of subjective probabilities is necessary and appropriate and provides a reasonable input to [assessing the risks of a nuclear reactor melting down]... It is true that a subjective probability is someone's opinion. But … some people's opinions can be very accurate, even in a quantitative sense".

Source: Ad Hoc Risk Assessment Review Group, *Risk Assessment: Review Group Report to the United States Nuclear Regulatory Commission* (September 1978).

After a realistic, manageable list of corruption vulnerabilities has been prepared, an estimate of the likelihood of the corruption occurring, and how much harm will result if it does, must be developed. No objective method exists for calculating either of these variables, but as box 6 explains, subjective estimates by informed observers can often be quite accurate.

At this stage, the working group should develop estimates for the likelihood and potential severity of each risk, based on their knowledge and the information available. Use of a limited number of descriptive words ("low", "medium", or "high", for example) is preferable to numerical estimates, as numerical estimates can create confusion, or overconfidence in their accuracy. Descriptive words are usually sufficient for prioritizing responses to different forms of corruption. When completing this step, group members should ensure that they share the same definition of the terms used.

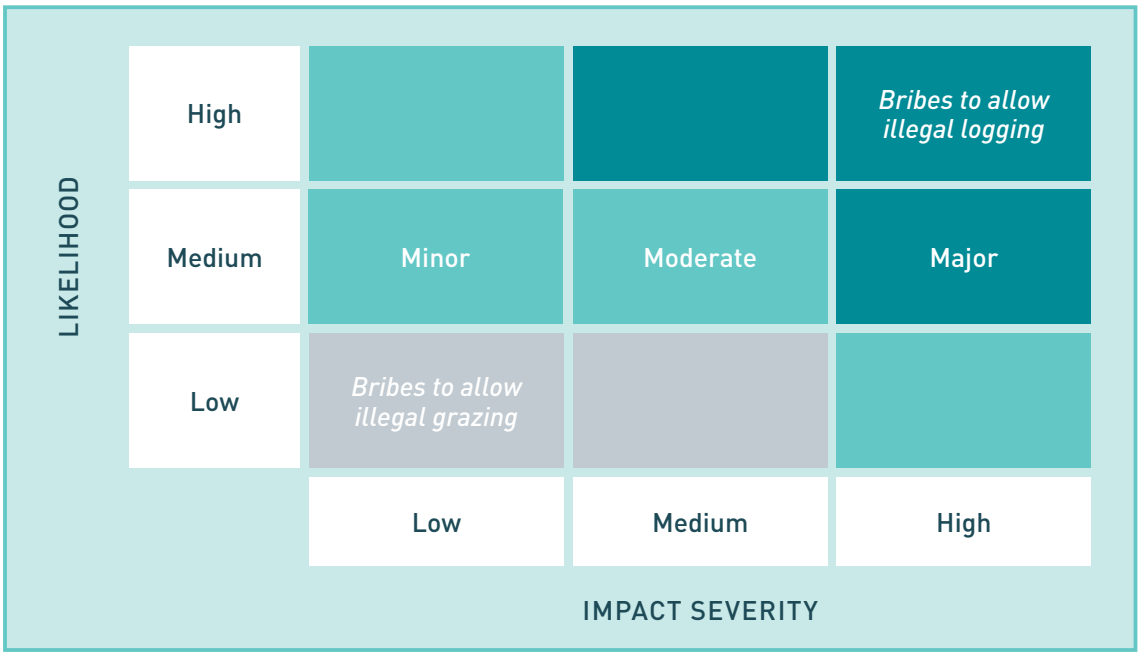
The same considerations apply when estimating the potential damage from different types of corruption. The working group needs to be clear about whether the estimate is limited to financial damage, or whether they are including other types of potential harm as well. The most common forms of non-financial damage considered when assessing corruption risks are the effects on the organization's reputation and its ability to fulfil its mandate. For example, while the economic loss incurred from a senior official falsifying a travel voucher might be small, the political consequences could be severe and public confidence in the organization could be badly damaged. Whether non-financial types of harm should be incorporated into the responses (and, if so, which ones), is a decision for the working group to make on the basis of the organization's situation and the environment in which it operates.

In this step, two separate estimates for each type of corruption risk (identified in step two of the risk assessment process) are developed: first, the likelihood of the risk's occurrence and second, the potential harm if that risk did occur. These estimates are then combined into a single measure showing which ones would pose the most serious threat to the organization if they were to occur. When the estimates for likelihood and harm are both in the form of "high", "medium" or "low", the most straightforward technique for combining them is to construct a three-by-three risk matrix with the rows listing likelihood and the columns denoting harm. Figure 2 is an example.

Risks in the three upper right-hand cells should all be considered major risks, as either the likelihood and severity are both "high", or one factor is "high" and the other is "medium" (darkest shading). Similarly, if both the likelihood and severity are "low", or one is "low" and the other is "medium", the risk is considered "minor" (lightest shading). Those falling in-between the two are ranked "moderate" (medium shading). Thus, by rating the likelihood and impact severity of identified risks, the working group can rank which of these risks should be addressed as a priority.

The types of corruption to which the organization is vulnerable can be put into the matrix as follows. Suppose the working group for the organization responsible for managing the nation's forests determines there is a risk that staff who oversee a protected reserve might take bribes to allow illegal logging on the reserve. Suppose also that the estimate of this form of corruption occurring is "high", and that reputational damage to the organization if it occurred would be "high" as well. The combination of high/high would put that risk in the upper right-hand of the matrix, in the cell labelled "Bribes to allow illegal logging".

Figure 2. Risk prioritization matrix



Assume a second risk identified in step two is that staff may occasionally allow neighbouring farmers to let their cattle graze in the reserve in return for small payments. The group concludes that the likelihood of this happening is "low" and that if it did, the damage to the organization's reputation and the economic loss would also be "low". The low/low combination puts it in the cell in the bottom left-hand corner, labelled "Bribes to allow illegal grazing".

When determining estimates of the likelihood that different forms of corruption schemes might occur, working group members should keep in mind various considerations. The questions outlined in box 7 can serve as a suitable starting point in this regard.

Box 7. Questions to estimate the likelihood of a corruption risk

- How complex is the potential corruption scheme, and how many people are required to perpetrate it?
- Have similar types of corruption occurred in the organization or in other government organizations?
- How much might those involved in such a scheme profit from it?
- How many other organization employees or officials in other organizations would have to look the other way for the scheme to succeed?
- Do internal procedures raise sufficient safeguards to deter those who would want to commit corrupt acts?

There is a potential pitfall associated with how people estimate the probability of future events. Research shows that when individuals are asked for probability estimates, they overestimate the likelihood of events with which they are familiar or which they can easily recall, and they underestimate or ignore those remote in time or experience, a cognitive bias known as the availability heuristic.[10] If there has been a recent case of bribery, or media accounts and policy discussions about corruption in the country have focused on bribery, there is a far greater chance estimators will identify bribery as more likely to occur and be more damaging

[10] Tversky, Amos; Kahneman, Daniel (1973). "Availability: A heuristic for judging frequency and probability". *Cognitive Psychology*. 5 (2): 207–232. DOI: 10.1016/0010-0285(73)90033-9. ISSN 0010-0285.

than other forms of corruption. Yet it may well be that other, less salient types of corruption, such as officials hiding their interests in a company bidding on a public contract, are in fact more likely to occur.

This bias can be countered. Those asked to offer estimates should be alerted to the issue and be mindful of it when offering their opinion. Questions can be injected into interviews and group discussions to minimize its effect, such as the following:

- Why does an interviewee or the group think one form of corruption is more likely to strike the organization than another?
- What factors lie behind this judgment?
- Are there any current corruption cases or issues currently prominent in the media that might affect discussions?

3.5 STEP 5 – PREPARING AND FINALIZING THE MITIGATION PLAN TO TREAT THE CORRUPTION RISKS

Step five of this process is the treatment of the identified and prioritized corruption risks through the development and implementation of a corruption risk mitigation plan. This plan describes the controls that the organization aims to implement in order to mitigate the potential corruption risks prioritized during the previous step. As mentioned above, controls are the policies, processes and management systems designed to prevent, deter and/or detect improper actions, thereby reducing the organization's risk. The plan must be detailed, with specific timelines that assign named personnel the responsibility for successfully implementing key actions and should be incorporated into the organization's operational and strategic workplans. This will help to ensure that funding and personnel needs are addressed. The process for developing the mitigation plan is described in detail below.

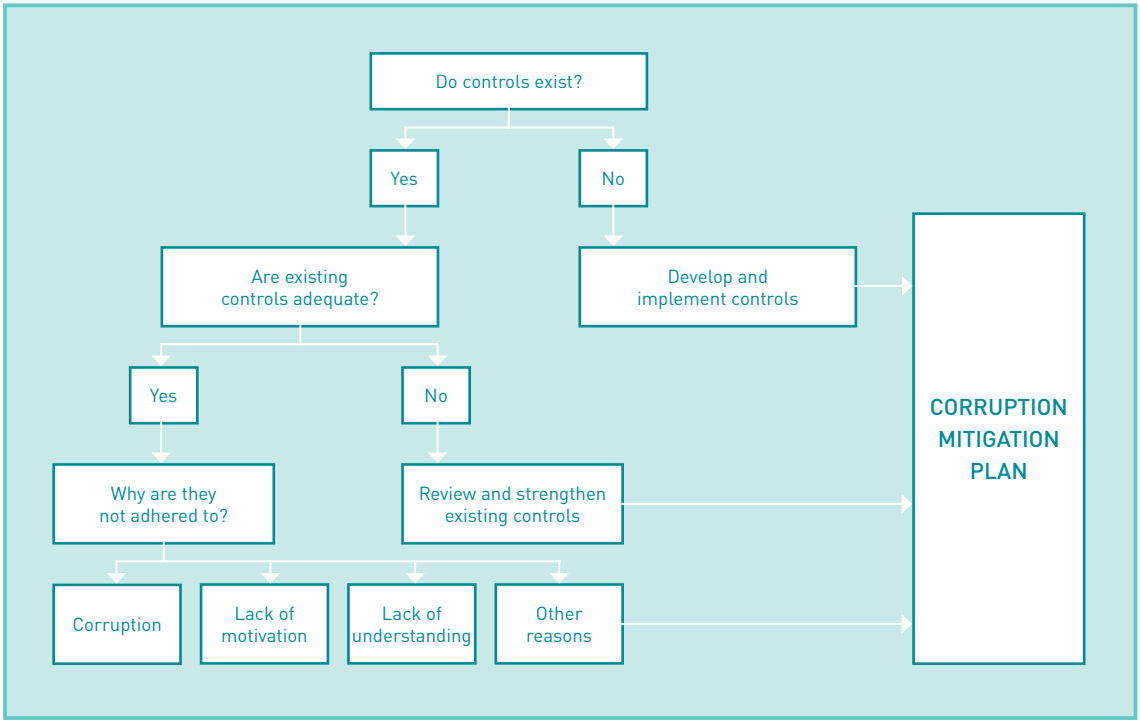
Review existing controls

All organizations have, or should have, procedures, rules and measures in place that aim to prevent and detect corruption. During the risk assessment process, the working group will have collected information on existing procedures within the institution. The working group must first identify the cause of particular corruption risks to determine which controls must be assessed and then analyse the extent to which such controls are effective. It is recommended that the working group follow the flow chart in figure 3 for each identified risk.

Take, for instance, an example from the field of procurement, in which the working group identifies that there is a potential risk associated with the overpayment of suppliers. The working group will need to determine the cause of that risk. It could be that there is a flaw in the procurement process allowing tenders with inflated prices to be selected, or suppliers may be submitting inflated invoices which, in turn, are not being properly checked. Once the working group identifies the cause of the risk, they can determine which controls must be assessed. If the problem is tenders with inflated prices, the working group may need to assess the entire pre-contract and contract stages of the tender process. Alternatively, if inflated invoices are being submitted, controls linked to the payment process may need to be examined.

Identifying where existing controls need strengthening will not always be obvious. The working group will have to make judgments about the effectiveness of existing controls. To do so, the working group can assign each control a grade of "effective", "moderately effective" or "not effective". Group members should agree on the criteria by which a process might be deemed "effective", "moderately effective" or "not effective". Guidance on how to examine the effectiveness of corruption prevention controls is provided by INTOSAI. It identifies eight key internal control activities critical to detecting and preventing corruption. The eight controls, along with INTOSAI guidance on how each should function, are presented in annex 4. It provides a useful tool for exploring how well any organization's internal control regime functions and offers criteria that group members can use to quantify why they gave a control a particular grade.

Figure 3. Risk prioritization matrix



The benefits of the review process (see figure 3) extend beyond the identification of risks and areas where controls need to be strengthened. They can also uncover, as box 8 illustrates, areas where controls are excessive and/or duplicative. When such unnecessary controls are identified, it is often the case that savings can be realized without any increase in overall corruption risk.

Box 8. Risk assessments can identify redundant controls

An evaluation of the fraud risks and existing controls within a government organization revealed that there were three separate control mechanisms to ensure that office equipment was not stolen. First, auditors conducted elaborate weekly inventories of all office equipment in the organization's headquarters building; second, the security division posted guards at every exit, who inspected all personnel and packages leaving the building; and third, the guards were monitored by closed-circuit cameras operated by a third party. The organization concluded that given these multiple, independent controls, the frequency and intensity of equipment audits could be reduced and audit resources were freed to examine other organizational operations.

Determine the need for and design additional controls

If the working group has found that an organization's control is moderately effective or not effective, the group will need to design additional controls.

A useful way to organize the working group's thinking is through a table listing each risk, the control or controls currently in place to mitigate it, a description of what risk remains, and what additional controls would help mitigate the remaining risk.

An example is shown in table 2. It has two rows: the first row assesses the risk that a firm supplying the organization with goods will fraudulently deliver a substandard product and the second row assesses the risk that the staff member in charge of inspecting the goods will take a bribe in return for approving payment for the substandard product. Examples of a product that fails to conform to the terms of the contract could be out-of-date pharmaceuticals, machinery that will not last as long as the contract requires or simply less printer paper being delivered than was ordered.

Existing mitigating provisions to avoid the fraudulent supply of substandard or nonconforming goods are usually in the contract between the organization and the supplier. These allow the organization to withhold payment or bring suit if the supplier fails to meet the contract terms. However, this can be difficult or impossible to enforce if the staff member responsible for receiving the product fails to notice the defective product and accepts the delivery. An additional control to reduce this risk is to assign one or more additional staff members to inspect the product before payment is authorized.

For the control to be meaningful, the additional reviewers must know what the contract requires and understand the product specifications. This is indicated in the "Additional controls" column of table 2. While checking a pharmaceutical package to ensure the expiration date has not passed is a straightforward task, examining a sample of the drug to be sure it has not been diluted or is not a fake requires a skilled technician with the appropriate equipment and training.

The second row of table 2 shows the existing controls in place to prevent a staff member from corruptly authorizing payment for a nonconforming or substandard good. These are the organization's ethics code and the national laws punishing bribery. The risk here is that the employee will ignore the code and the law, thinking he or she will not get caught, or (as discussed below) that his or her actions are justified. Therefore, the cell in the second row under "Additional controls" proposes three controls to reduce this corruption risk: additional inspections by knowledgeable staff, checking the staff member's lifestyle to see if he or she is living beyond his or her means, and third, visiting the supplier's office or facility unannounced.

Table 2. Assessing the control environment

RISK	EXISTING CONTROLS	REMAINING RISK	ADDITIONAL CONTROLS
Nonconforming product delivered	Penalties in procurement contract	Staff receiving product fails to notice irregularity	Other staff knowledgeable about the product and the contract inspect the delivery
Staff receiving product bribed to approve nonconforming product	Ethics code Antibribery law	Staff member ignores law and code	Additional, knowledgeable staff inspect product Receiving staff member's lifestyle assessed Unannounced visits to facility or supplier's office

Which of these are appropriate will depend upon circumstances. If the fear is that lower-level staff will accept fewer boxes of paper or a lesser number of office chairs and tables than the contract requires, additional inspections may be all that is required. If the contract is for costly equipment, involving a firm that might be willing to pay a significant bribe to deliver a substandard product, a lifestyle assessment might also be in order. Furthermore, in the case of pharmaceuticals, an unannounced visit to the manufacturing or packaging facility could be useful in revealing signs that the supplier diluted or falsified a drug.

Consider the availability and feasibility of external control mechanisms

External controls, such as mechanisms for public transparency and external review of the organization's policies and decisions, can complement internal activities. Such controls could consist of publishing information on the organization's profits, spending patterns and governance, affording external stakeholders the opportunity to view and analyse the data. Monitoring conducted by civil society groups and independent institutions could track the organization's planned activities, financial flows and/or adherence to legal requirements, thereby identifying any gaps or suggesting useful recommendations. External controls could also include cooperative multi-stakeholder groups within the organization's particular sector that agree to the same minimum standards of public transparency and work together to hold each other accountable.

Addressing individual risk

In addition to the organization's procedural controls, the working group should consider assessing staff for corruption risks. The organization could have sufficient controls in place to mitigate the prioritized corruption risks, but if staff do not understand how to use and manage those controls or are not motivated to follow internal procedures, corruption risks may still exist. While this guide does not suggest profiling employees, it is important to understand that some employees are in positions where the risk of them being exposed to corruption is greater than others. It may be necessary to create additional controls relating to such employees, such as regular asset declarations.

Figure 4 shows the individual risk factors for corruption.[11] These factors include opportunity (access to resources, decision-making, position of power), perceived pressure (greed or actual need for money) and rationalization (explaining to oneself how the illegal behaviour is compatible with one's own standards of conduct and is justified under the circumstances).

Figure 4. Individual risk factors for corruption

(a) Opportunity

Officials are only able to embezzle if they have access to or control of the assets that they are exploiting. Similarly, they are only able to influence a decision if they have decision-making powers or are advisers to decision makers. Simply, individuals can only commit corruption if they are in a position to do so.

Therefore, as the United Nations Convention against Corruption suggests, it is always advisable to take special measures to ensure the integrity of staff who hold sensitive positions. These measures may include specialized training, restrictions on external interests, or disclosure requirements. There may also be a requirement for additional or enhanced vetting at regular intervals.

(b) Pressure

Opportunity alone is not enough to explain why officials engage in corruption. After all, there are millions of civil servants with access to assets or with decision-making powers who are perfectly honest. The second important factor is pressure. This could be a real or perceived need, or pressure from relatives, colleagues, criminals or acquaintances.

[11] Donald Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement* (1953).

The pressure may come in the form of actual need (for example, money needed to pay for expensive medical treatment or a child's education, or to supplement a missed salary payment), perceived need (for example, the "need" to buy an expensive watch or car to impress clients) or greed (for example, money needed to maintain an expensive hobby).

(c) Rationalization

Most officials involved in corruption are people who have made a series of wrong decisions, leading to a final mistake that brings about their detection. They rarely perceive themselves as criminals; instead, they try to rationalize or justify their behaviour. Feelings of frustration, revenge or disloyalty, or that they are being mistreated and are not receiving what they are entitled to, are all powerful enablers of corruption.

Assess the feasibility of additional controls

Many organizations have limited resources and may still be developing a consensus on how and whether to address certain corruption risks. The working group must therefore consider whether the proposed new controls are both affordable and feasible. While assigning a second employee to visit a job site may not be expensive, it is not costless either. The organization would have to consider transportation expenses, along with the employee's time away from other duties. If the job is located a considerable distance away, perhaps a day's journey or more, an organization with limited resources may find the cost of transport, accommodation and subsistence prohibitive.

In addition to ensuring measures are affordable, the working group must also ensure they are feasible. Examples of expensive and difficult measures include a major political or institutional reform, or changes in the nation's laws or its constitution. Although these measures may address a certain risk, they are so costly in terms of resources (time, political capital and public support) that the respective organization would instead find itself engaged in a lengthy and expensive battle that would impact its ability to carry out its primary function.

Realistic controls should be specific and clear, and not cost more than the damage that would result from a particular corruption risk occurring. In a case where corruption exists on a construction site, while it might be too costly or unfeasible for another employee to conduct additional oversight, it might be possible to enlist someone from an external anti-corruption organization to periodically visit the location to review documents and gauge progress. Where public interest in the construction project is high, the organization might arrange for the media or civil society organizations to regularly visit the site and report on progress.

Another practice is to think in advance about the potential problems and challenges in the implementation of the proposed measures. Such an analysis would help to anticipate any major issues and identify those measures which are either unfeasible, too broad in scope or too expensive (in terms of costs, political capital or administrative resources).

Finalize and adopt the mitigation plan

Before finalizing the plan, the working group will want to discuss it with the organization's personnel and stakeholders, after which it should then obtain the approval of senior management. The plan should outline the key measures and actions that the organization will implement to mitigate the corruption risks identified during the previous steps. As table 3 illustrates, a detailed plan will contain clear timelines for the implementation of controls, including new measures, and will identify and record the unit responsible, along with a named individual for every action outlined in the plan. The working group should also include mandatory reporting and oversight mechanisms to ensure that the plan is delivered.

Table 3. Sample risk mitigation plan

RISK MITIGATION ACTION	SPECIFIC ACTIONS	RESPONSIBILITY	RESOURCES	TIMELINE
Computerize system from pre-contract to award of tender.	Agree on scope of the system Determine if a bespoke system is required, or an existing system can be used Develop and test the system	Director, Information Technology, Ministry of Construction	Consider the personnel, time and financial resources needed to implement the action	31 August XXXX 30 September XXXX 30 November XXXX
Create strict process for approving changes in tenders.	Develop and agree on a new system for chain of approvals Communicate new system to relevant staff Test the system to ensure it is feasible and efficient	Director of Operations, Ministry of Construction	Consider the personnel, time and financial resources needed to implement the action	31 August XXXX 30 September XXX 30 September – 1 November XXXX
Embed a red flag system to identify potential anomalies in the application and award of tenders.	Develop and agree on criteria that will indicate potential abuse of the system Agree on a system whereby internal control receives system-generated red-flag reports	Deputy Director General, Ministry of Construction	Consider the personnel, time and financial resources needed to implement the action	31 August XXXX 30 November XXXX

Incorporate the mitigation plan into the organization's operational and strategic workplans

To ensure that the organization commits sufficient time and funds to implement the corruption risk mitigation plan, it should incorporate the plan into broader operational and strategic workplans under the supervision of key personnel who are responsible for its success. This will ensure that funds are appropriately sourced and allocated, especially if resources are not immediately available, and that personnel with relevant skills are tasked with implementing the newly identified controls.

Implement the plan

Finally, once the plan has been approved, it should be delivered. Information that might help those trying to avoid detection should remain confidential. Otherwise, the plan should be published. Publication will reaffirm the organization's commitment to implementing the plan and will also allow parliament, auditors and the public to monitor the organization's success in doing so.

Monitor and evaluate the implementation of the plan

Specific indicators should be developed for each risk and corresponding mitigation measure to enable the organization to monitor and evaluate whether each measure is successful and, if not, to adjust its mitigation plan. Indeed, the mitigation measures identified in the plan should be monitored for effectiveness and, along with any outstanding or newly emerging corruption risks, should be fed back into a cycle of risk assessment

and management (see section 2.6, "Creating feedback mechanisms"), making adjustments to the process, infrastructure and capacity as necessary. Over time, this cycle can embed a culture of integrity and support organizations in achieving "transparency and accountability in the management of public finances", as is promoted by the United Nations Convention against Corruption.[12]

[12] UNODC, *United Nations Convention against Corruption* (2004), art. 9, para. 2*(d)*, p. 13.

Chapter 4.

CONCLUSION

Public sector organizations with limited resources are able to more effectively use those resources to address and reduce corruption if they follow a process of risk assessment and management. Taking this approach, organizations can focus on implementing realistic measures that reduce the risk of the most likely and most damaging corruption schemes causing the organization financial or reputational damage or impacting its ability to achieve its mandate.

To support the success of the risk assessment process, a working group should be appointed, comprised of organizational staff with a broad range of knowledge and expertise, and backed by the highest authority possible. The working group may benefit from external consultants in cases where experience or expertise may be lacking, or where staff are reluctant to discuss corruption candidly for fear of retaliation from colleagues.

Throughout the process, efforts should be made to emphasize that the corruption risk assessment is not a witch-hunt. The purpose of the assessment is not to flush out individuals that *have* engaged in corruption, but instead to highlight any organizational vulnerabilities that *could* provide opportunities for corruption to take place. The purpose of the risk mitigation plan is to then reduce these opportunities and either introduce or strengthen controls and measures that lessen the organization's vulnerabilities.

In accordance with ISO 31000 principles, this guide suggests that organizations, through the appointed working group, undertake the structured step-by-step risk assessment and management process shown in table 4.[13]

[13] ISO, *ISO 31000:2018, Risk management — Guidelines*.

Table 4. Step-by-step risk assessment and management process

Step 1. Establish context	Evaluate the operating environment of the organization, including mandates, functions and stakeholders
Step 2. Identify risks	List possible corruption schemes and scenarios
Step 3. Analyse risks	Review internal documents, controls and records to assess the probability of identified risks
Step 4. Evaluate risks	Assess the likelihood and impact of corruption risks, prioritize them and address major risks first
Step 5. Treat risks	Review existing controls, determine the need for, and feasibility of, new controls, and prepare and deliver the risk mitigation plan

While conducting the risk assessment process, and in order to most effectively use limited resources to reduce corruption, public organizations should focus their efforts on the highest priority risks (the most likely and most damaging) and the most practical mitigation measures (the most feasible and affordable).

By monitoring and reviewing both the delivery and the effectiveness of the risk assessment and mitigation plan, improvements can be made to the process and measures may be revised. This guide advises that public organizations should repeat the process regularly and embed risk management within their standard operations to ensure that they can respond to the constantly evolving risks of corruption that they face, thus contributing to the achievement of the Sustainable Development Goals, including Goal 16 and target 16.5, which aim to "substantially reduce corruption and bribery in all their forms".[14]

[14] "Transforming our World: the 2030 Agenda for Sustainable Development" (General Assembly resolution 70/1), Sustainable Development Goals and targets, Goal 16; see also https://sustainabledevelopment.un.org/sdg16.

Annexes

1. THE HISTORY AND INTERNATIONAL CONTEXT OF CORRUPTION RISK MANAGEMENT

Modern corruption risk management programmes are rooted in the need for all organizations, both public and private, to anticipate and, where possible, prevent events that might be to the detriment of the public, erode faith in public institutions, or prevent organizations from achieving their mandates. This involves, but is not limited to, the manifestations of corruption listed in chapter 1.

A major milestone in the effort to systematically assess fraud and corruption risks faced by organizations was the move in the 1990s to strengthen internal control systems in both public organizations and private corporations. A number of cases from the 1970s, 1980s and 1990s had demonstrated the inadequacy of existing regulations in preventing large-scale fraud, and so in 1992 the Committee of Sponsoring Organizations of the Treadwell Commission (COSO)[1] published a four-volume report containing guidance on what an adequate system of corporate internal control should include.

That same year, the International Organization of Supreme Audit Institutions (INTOSAI) issued new standards for the internal control of public organizations. Both the COSO and the INTOSAI guidelines recommended that internal auditors estimate the probability of an organization falling victim to fraud and offered advice for management personnel on steps that might reduce those chances.

While the COSO and INTOSAI guidelines both provide recommendations on best practices that, when implemented, can reduce the chances of fraud, their status as voluntary recommendations inevitably reduced their impact. They did not, and still do not, by themselves compel any organization, public or private, to have a corruption risk assessment and management plan.

However, with the entry into force of the United Nations Convention against Corruption in December 2005, the domestic legal requirements and regulations regarding corruption were further strengthened. Article 9 of the Convention introduced a mandatory provision for States parties to establish "effective and efficient systems of risk management and internal control" as a means for promoting "transparency and accountability in the management of public finances".[2]

The Convention also created powerful incentives for both public and private organizations to implement corruption risk assessment and management programmes. States parties were now required to hold corporations responsible for participating in the corrupt acts of their employees, and many countries have since

[1] For more information, see www.coso.org/Pages/aboutus.aspx. COSO was founded in 1985 by the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors and the National Association of Accountants (now the Institute of Management Accountants).

[2] United Nations Convention against Corruption, art. 9, para. 2*(d)*.

enacted legislation allowing a corporation to avoid liability for employee corruption only if it can show it has carried out a corruption risk assessment and has implemented adequate procedures to mitigate the risks identified.

International and national examples include:

- The Convention on Combating Bribery of Foreign Public Officials in International Business Transactions states that "each Party shall take any measures necessary to establish that complicity in, including incitement, aiding and abetting, or authorization of an act of bribery of a foreign public official shall be a criminal offence".[3]
- The United States Corporate Enforcement Policy states that, "when a company has voluntarily self-disclosed misconduct in a Foreign Corrupt Practices Act matter, fully cooperated, and timely and appropriately remediated," all in accordance with the required standards, then the Fraud Section will "accord, or recommend to a sentencing court, a 50 per cent reduction off of the low end of the United States Sentencing Guidelines fine range, except in the case of a criminal recidivist; and generally will not require appointment of a monitor if a company has, at the time of resolution, implemented an effective compliance program".[4]
- In the United Kingdom, the Bribery Act of 2010 states that "a relevant commercial organization ('C') is guilty of an offence under this section if a person ('A') associated with C bribes another person intending *(a)* to obtain or retain business for C, or *(b)* to obtain or retain an advantage in the conduct of business for C. (2) But it is a defence for C to prove that C had in place adequate procedures designed to prevent persons associated with C from undertaking such conduct".[5]

With near universal ratification of the United Nations Convention against Corruption, the number of public and private entities looking to implement a corruption risk assessment and mitigation plan is substantial, and with this growth in demand has come an explosion of books, articles and brochures focusing on this topic.[6] These publications cater primarily to private sector demand and focus on bribery, the principal corruption risk faced by private firms.

Guides for public sector organizations are often very different to those written for the private sector, including in terms of form, terminology and the sequence of steps suggested when assessing corruption risks.

The methodologies outlined in the public sector-focused publications are broadly based on the concept of enterprise risk management (ERM),[7] a process designed to systematically evaluate the risks faced by a particular organization in order to develop a mitigation plan. The COSO ERM methodology has, over time, become the international standard for effective risk management best practice, and forms the foundation for International Standards Organization (ISO) standards such as *ISO 31000:2018, Risk Management – Guidelines.*[8]

These ERM methodologies can often result in extensive, detailed and therefore lengthy risk management processes. It is assumed that the organization has the required resources, capacity and time to conduct the assessment, that the assessment will identify all risks of corruption to which the organization is exposed and that the organization has sufficient resources to address these risks. These methodologies also assume that the organization operates in (and encourages) an environment in which addressing corruption is an undisputed priority.

However, as mentioned previously, many public organizations lack the necessary resources, capacity or time to carry out such an extensive programme of risk management.

[3] Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, art. 1, para. 2. Available at www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf.

[4] United States Foreign Corrupt Practices Act Corporate Enforcement Policy (United States Attorney's Manual 9-47.120), art. 1. Available at www.justice.gov/criminal-fraud/corporate-enforcement-policy.

[5] United Kingdom Bribery Act 2010, art. 7, para. 1. Available at www.legislation.gov.uk/ukpga/2010/23/pdfs/ukpga_20100023_en.pdf.

[6] Annex 2 lists some of the most frequently cited publications on the topic.

[7] See www.coso.org/Pages/erm-integratedframework.aspx.

[8] For more details on the ISO 31000 standard, please see annex 3.

2. FREQUENTLY CITED CORRUPTION RISK ASSESSMENT GUIDES

The inclusion of references to the following corruption risk assessment guides and their contents do not necessarily reflect the views or policies of the United Nations Office on Drugs and Crime, Member States or contributory organizations, and neither do they imply any endorsement.

ACL, *Bribery and Corruption: The Essential Guide to Managing the Risks* (ACL, 2015).

Arnold and Porter, *Building an Effective Anti-Corruption Compliance Program: Lessons Learned from the Recent Deferred Prosecution Agreements in Panalpina, Alcatel-Lucent, and Tyson Foods* (March 2011).

Bertram I. Spector, Michael Johnston, and Svetlana Winbourne, *Anticorruption Assessment Handbook* (United States Agency for International Development, 2009).

Carsten Giersch, *Corruption Risk Assessment Tool for the European Economic Area and Norway Financial Mechanism: 2009–2014* (September 2012).

Ernst and Young, *Building a Robust Anti-Corruption Program: Seven Steps to Help You Evaluate and Address Corruption Risks* (2010).

European Commission, *European Structural and Investment Funds, Guidance for Member States and Programme Authorities, Fraud Risk Assessment and Effective and Proportionate Antifraud Measures* (June 2014).

Gusztáv Báger, "Corruption Risks in Public Administration: Methodology and Empirical Experiences", *Public Finance Quarterly*, vol. 56, No. 1 (2011), pp. 44–57.

Institute of Internal Auditors, American Institute of Certified Public Accountants and Association of Certified Fraud Examiners, *Managing the Business Risk of Fraud: A Practical Guide* (2010).

Jesper Stenber Johnsøn, *The Basics of Corruption Risk Management: A Framework for Decisionmaking and Integration into the Project Cycles* (U4 Anti-Corruption Resource Centre, December 2015).

Karlyn D. Stanley, Elivara N. Loredo, Nicholas Burger, Jeremy N.V. Miles, Clinton W. Saloga, *Business Bribery Risk Assessment* (Rand Corporation for TRACE International, 2014).

Matt Morley, *How to Perform a Corruption Risk Assessment* (LexisNexis, May 2013).

Mohammed Ahmed and Robert Biskup (Deloitte), *The Necessary Steps Companies Need to Take in Conducting Anti-Corruption Risk Assessments* (Ethisphere, 2013).

Navex Global, *A Definitive Guide to Compliance Program Assessment and Anti-Bribery and Corruption Risk Assessment Checklist* (no date).

Nitish Singh and Thomas Bussen, *Compliance Management: A How-to Guide* (Praeger, 2015).

PWC, *Assessing the Risk of Bribery and Corruption to Your Business* (PWC, 2016).

Standards Australia, *Fraud and Corruption Control: AS 8001–2008, 2nd edition* (Standards Australia, 2008).

U4 Anti-Corruption Resource Centre, *Overview of Corruption Risk Management Approaches and Key Vulnerabilities in Development Assistance* (U4 Anti-Corruption Resource Centre, June 2016).

United Nations Development Programme, *Corruption Risk Assessment and Integrity Planning: Preventive Measures for Addressing Corruption in Nigeria* (United Nations Development Programme Nigeria, 2016).

United Nations Global Compact, *A Guide for Anti-Corruption Risk Assessment* (United Nations, 2013).

GUIDES FOCUSED ON PUBLIC ORGANIZATIONS

Council of Europe, *Corruption Risk Assessment Methodology Guide* (December 2010).

Hans Benner and Ina de Haan, *SAINT: A Tool to Assess the Integrity of Public Sector Organizations* (International Journal of Government Auditing, 2008).

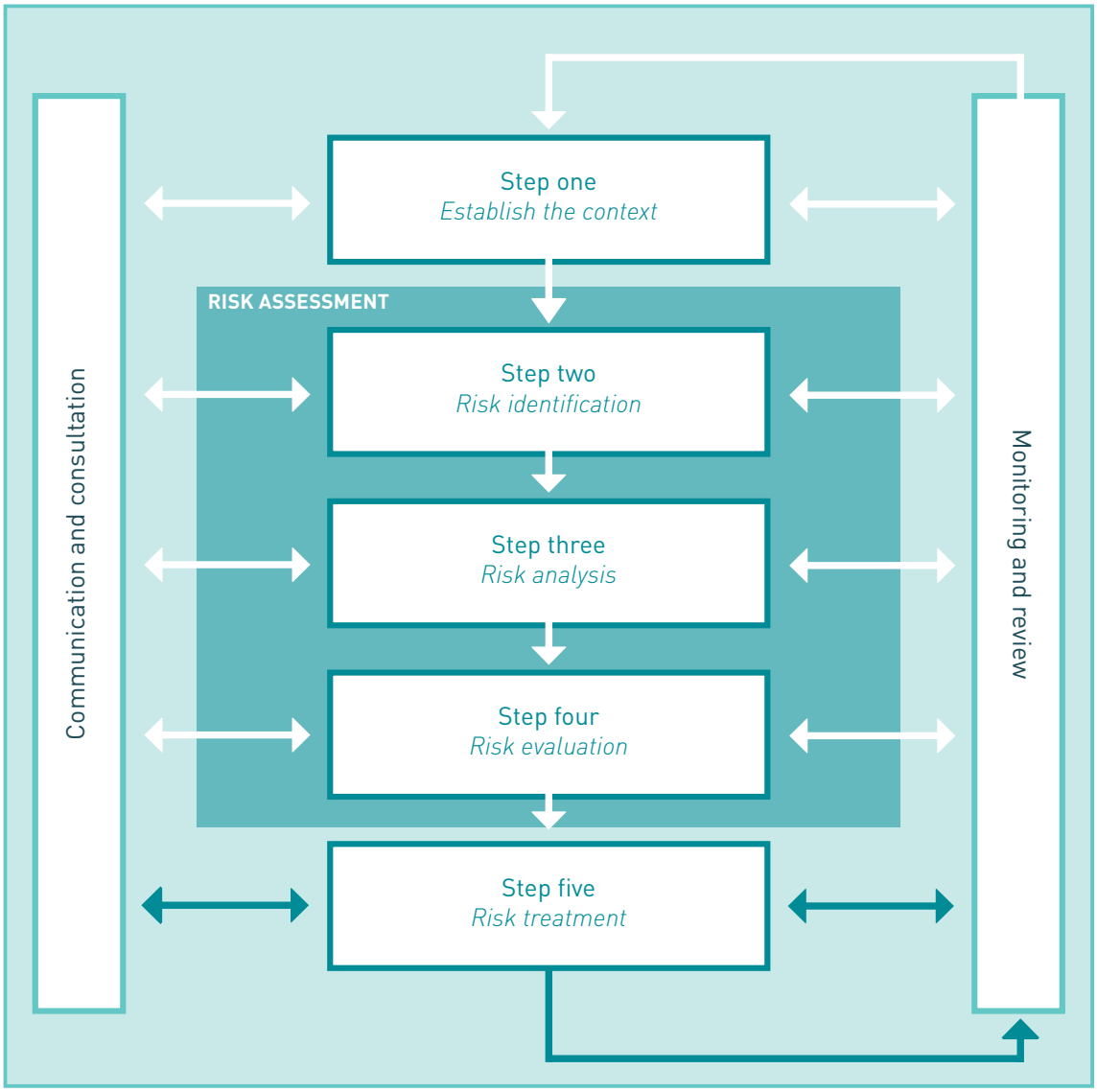
Liljana Selinšek, *Corruption Risk Assessment in Public Institutions in South Eastern Europe: Comparative Research and Methodology* (Regional Cooperation Council, 2015).

U4 Anti-Corruption Resource Centre, *Corruption Self-Assessment Tools for the Public Sector* (November 2016).

3. ENTERPRISE RISK ASSESSMENT

In 2009, the International Standards Organization promulgated a revised version of ISO 31000:2018, *Risk Management – Guidelines,* the current, authoritative guide to conducting organization or enterprise-wide risk assessment and management programmes. As the figure below shows, the process consists of five separate steps:

Risk assessment and management process



Step one requires the organization to "establish the context". The context includes the organization's mission, the rules governing its operation, the factors affecting its operation, and its ability to meet its objectives.

In step two, "risk identification", the various events that could occur in the future and interfere with normal operations are listed.

Step three, "risk analysis", requires estimating how likely it is for these events to occur. For example, if certain corruption schemes have taken place in the past, risk analysis aims to predict the likelihood of these schemes being used again.

Step four, "risk evaluation", estimates the impact of these future events, for example, in terms of financial loss or reputational loss in the case of a corruption scandal.

Steps two, three and four, contained within the dark shaded background in the diagram, are grouped together as "risk assessment" per se, to set them off from the fifth step, which ISO 31000 terms "risk treatment". Risk treatment, called "plan development" in corruption risk assessment and management terms, consists of the actions taken to address the risks; in other words, the development and implementation of a risk mitigation plan. In this step, the effectiveness of existing precautions and the need for additional ones are assessed. When assessing the corruption risk, the analysis would quantify the likelihood that a corruption risk would occur and the costs of possible measures to prevent it. This also includes an analysis of the management structure and internal responsibilities in case a risk occurs.

The boxes to the left and right of the figure are labelled "communication and consultation" and "monitoring and review" respectively. In combination with the five steps, they constitute what ISO 31000 terms the risk management process. The model emphasizes participation and communication with stakeholders and underlines that the risk assessment is a process and not a one-time event.

"Communication and consultation" also include documenting the work at each step and ensuring that both the organization's stakeholders and its leaders are informed. Constant communication and consultation not only ensure that nothing is overlooked but also further accountability and increase the chances that the resulting "treatment", or plan for managing the risks, will be implemented.

"Monitoring and review" shows that risk assessment and management is a continuing activity and not merely a one-time event, and that at every stage the information needed for the next step should be gathered and fed back into the process. This increases the chances that the mitigation measures will be implemented. "Monitoring and review" are important components of the risk management process. The world changes – new threats are appearing – and it is therefore important that, once the identified and prioritized risks are addressed, the organization reviews the risks that for whatever reason were not prioritized, and establish whether new risks have emerged.

4. INTERNAL CONTROLS TO DETECT AND PREVENT FRAUD

1. *Authorization and approval procedures.* Authorizing and executing transactions and events are only done by persons acting within the scope of their authority. Authorization is the principal means of ensuring that only valid transactions and events are initiated as intended by management. Approval procedures, which should be documented and clearly communicated to managers and employees, should include the specific conditions and terms under which authorizations are to be made. Conforming to the terms of an authorization means that employees act in accordance with directives and within the limitations established by management or legislation.

2. *Segregation of duties (authorizing, processing, recording and reviewing).* To reduce the risk of error, waste or wrongful acts, as well as the risk of not detecting such problems, no single individual or working group should control all key stages of a transaction or event. Rather, duties and responsibilities should be assigned systematically to several individuals to ensure that effective checks and balances exist. Key duties include authorizing and processing transactions, recording, and reviewing or auditing transactions. Collusion, however, can reduce or destroy the effectiveness of this internal control activity. A small organization may have too few employees to fully implement this control. In such cases, management must be aware of the risks and compensate with other controls. Rotation of employees may help ensure that one person does not deal with all the key aspects of transactions or events for an undue length of time. Encouraging or requiring annual holidays may also help reduce risk by bringing about a temporary rotation of duties.

3. *Controls over access to resources and records.* Access to resources and records is limited to authorized individuals who are accountable for their custody or use. Accountability for custody is evidenced by the existence of receipts, inventories, or other records assigning and recording the transfer of custody. Restricting access to resources reduces the risk of unauthorized use or loss to the government and helps achieve management directives. The degree of restriction depends on the vulnerability of the resource and the perceived risk of loss or improper use and should be periodically assessed. When determining an asset's vulnerability, its cost, portability and exchangeability should be considered.

4. *Verifications.* Transactions and significant events are verified before and after processing; for example, when goods are delivered, the number of goods supplied is verified against the number of goods ordered. Afterwards, the number of goods invoiced is verified against the number of goods received. The inventory is also verified by performing stocktaking.

5. *Reconciliations.* Records are reconciled with the appropriate documents on a regular basis; for example, the accounting records relating to bank accounts are reconciled with the corresponding bank statements.

6. *Reviews of operating performance.* Operating performance is reviewed against a set of standards on a regular basis, assessing effectiveness and efficiency. If performance reviews determine that actual accomplishments do not meet established objectives or standards, the processes and activities established to achieve the objectives should be reviewed to determine if improvements are needed.

7. *Reviews of operations, processes and activities.* Operations, processes and activities should be periodically reviewed to ensure that they follow current regulations, policies, procedures or other requirements. This type of review of the actual operations of an organization should be clearly distinguished from the monitoring of internal controls.

8. *Supervision (assigning, reviewing and approving, guidance and training)*. Competent supervision helps to ensure that internal control objectives are achieved. Assigning, reviewing and approving an employee's work encompasses the following:

- Clearly communicating the duties, responsibilities and accountabilities assigned to each staff member
- Systematically reviewing each member's work to the extent necessary
- Approving work at critical points to ensure that it flows as intended

A supervisor's delegation of work should not diminish the supervisor's accountability for these responsibilities and duties. Supervisors must also provide their employees with the necessary guidance and training to help ensure that errors, waste and wrongful acts are minimized and that management directives are understood and achieved.

The above list is not exhaustive but enumerates the most common preventive and detective control activities. Control activities 1 to 3 are preventive, 4 to 6 are more detective, while 7 and 8 are both preventive and detective. Entities should reach an adequate balance between detective and preventive control activities, whereby a mix of controls is used to compensate for the disadvantages of individual controls.

Once a control activity is implemented, it is essential that assurance of its effectiveness is obtained. Consequently, corrective actions are a necessary complement to control activities. Moreover, it must be clear that control activities form only one component of internal control and should be integrated with the other four components. We refer the reader to the annexes for integrated examples of each of the objectives and components of internal control.

Source: Excerpt from International Organization of Supreme Audit Institutions (INTOSAI), *INTOSAI GOV 9100, Guidelines for Internal Control Standards for the Public Sector.*

5. HOW BRIBES CAN BE PAID TO PUBLIC EMPLOYEES

A public employee who asks for or receives money, anything else of value or any undue advantage in return for doing an official act or refraining from acting in the exercise of his or her official duties has committed the offence of "passive bribery". The bribe need not go straight to the employee; it can be routed through a third person.

The bribe can take many forms:

- The use of credit cards, cars or aeroplanes at no charge or at a discount
- An ownership interest in a company at a discount
- A kickback, a secret payment after a transaction with the government is completed
- An opportunity to purchase something at a discount
- A loan that is later forgiven or repaid at a discount or extended at a rate less than the market rate of interest
- Support for expensive hobbies such as collecting rare stamps or coins
- Payment of expenses, often the tuition of a child attending a school overseas
- Meals, entertainment, vacations or other gifts
- Sexual favours

VARIATIONS

- Something of value received IN ADVANCE to do something which is NOT a crime
- Something of value received IN ADVANCE to commit a crime
- Something of value received EX POST for doing something which is NOT a crime
- Something of value received EX POST for committing a crime (a "tip" or "gratuity" for services performed)
- Regular transfers of something of value, usually money, without an expectation for a specific action (as "retainer")

EXAMPLES OF "SOMETHING OF VALUE"

Direct: money, favours, preferential treatment, access to clubs, discounts, entertainment (tickets, sexual services, parties), transfer of property (movable, real estate), transfer of shares of companies, payment of expenses, in-kind gifts of any value intended to influence the public official, access to limited resources.

Indirect: usually concealed through a legitimate transaction, such as fees for publishing books; per diems for participation in events; large speaking fees; business opportunities through companies with ties to a public official or of which the public official is a beneficial owner, even when the prices are not inflated; payment of costs for education or health care; holidays, indirectly – through intermediaries; loans with preferential interest rates or loans which are never meant to be repaid; allowing the use of resources (for example, a car that an official could use as his or her own, a house or vacation home, computers, mobile phones, etc.)

6. EMBEZZLEMENT SCHEMES

Embezzlement is the theft or misappropriation or other diversion or misuse by a public employee, for his or her benefit or for the benefit of another person or entity, of:

- Any property
- Public or private funds or securities
- Any other item of value entrusted to the public official by virtue of his or her position

The theft or embezzlement can be accomplished in various ways:

- *Cash skimming.* Collecting cash and either:
  - Not reporting it, or;
  - Underreporting it, or;
  - Holding it temporarily in his or her own account to generate interest.

  The money may be skimmed when payments are collected from citizens in cash. The payments may be for fines, licences, permits, fees or any other kind of cash received by a public sector organization.
- *Cheque fraud.* Rare in most of the world but may take place where cheques are used extensively. Examples include:
  - Forging an authorized signature
  - Forging an endorsement signature
  - Changing the payee designation
  - Directly (when authorized) issuing cheques to oneself
- *Billing schemes.* Invoices from fictitious companies submitted for payment. For example, an employee submits an invoice for fumigation or cleaning services performed by the XYZ company, a fake company the employee created.
- *Overpayment schemes.* For example, the invoice for a stay at a hotel amounts to $100 and the employee adds two zeroes to make it $10,000 and splits the overcharge with the hotel. An employee may also change the bank account number of an established supplier so that payments are sent to the new, fraudulent account rather than the supplier's actual account.
- *Personal purchases.* An employee submits for reimbursement an invoice for a personal purchase. For example, fuel used for the employee's own vehicle rather than a government car.
- *Payroll fraud:* This often requires the involvement of several employees. One or more individuals are placed on the payroll who never show up for work ("ghost employees"). Alternatively, employees work but are overpaid by misrepresenting the hours worked or the tasks performed.
- *Misuse of property:* For instance, a government car is used for personal errands.

7. EXPENSE REIMBURSEMENT FRAUD

An auditor working on an expense reimbursement audit at a public organization noticed that one individual submitted requests for reimbursement for exam/certification costs for accounting training five times within a year. This seemed unusual to the auditor because he knew how much time it takes to prepare for the exams associated with the accounting profession. For the review, the auditor requested the supporting documentation required for reimbursement.

The supporting documentation included receipts and notices of pass/fail that were in email format, leading the auditor to believe that the employee simply created fictitious expenses which the employee asked his organization/employer to pay for. Also, upon interviewing the employee, the auditor discovered the employee could not produce the actual certificates nor prove he was required to take the courses as part of his job.

An inquiry with the organization confirmed that reimbursement requests did not require a manager's review and approval and the organization did not maintain a list of the employees seeking reimbursement for certification costs. Once an employee submitted a reimbursement package, the package was simply stored in a filing cabinet.

The auditor determined that the employee was successful in producing authentic-looking counterfeit email receipts using graphic software on his personal computer. The case was referred to the anticorruption organization for further investigation.

LESSONS LEARNED

In expense reimbursement schemes, employees simply create fictitious expenses that they then ask their employers to pay. They can accomplish this by producing authentic-looking counterfeit receipts, emails, etc., using graphic software on their personal computers. Lack of controls, absence of management review and overrides of existing controls are cited as the most common factors enabling expense reimbursement schemes.

FRAUD INDICATORS

- Multiple requests for reimbursement for certification costs within a specific time frame
- Absence of management review for reimbursement packages
- Failure to maintain a list of the employees who seek reimbursement for certification costs

8. EXAMPLES OF CONFLICTS OF INTEREST

A conflict of interest occurs whenever a public employee places his or her own interests or those of a relative, friend or business associate over the public interest. Examples include the following:

- Assistance provided by an individual or firm in their dealings with the government; for example, representing someone in a lawsuit or claim against a government ministry.
- An award by the public servant of a government contract to him- or herself or a close relative or friend, the issuance of a decision affecting his or her business or property or that of a close relative or friend, or other instances where a public servant acts for both the government and him- or herself or a close relative or friend in a transaction.
- Acceptance by a public employee of compensation from someone outside the government for performing his or her duties.
- A former public employee providing advice, after leaving government service, to an individual or company on a matter the former employee worked on while in government.

9. CONFLICTS OF INTEREST IN PROCUREMENT: SIGNS AND CONTROLS

Example

An employee from a public institution defrauded his employer by purchasing items from a certain vendor at inflated prices. The vendor firm was owned by his wife and run by his brother-in-law. The employee's interest in the company was not disclosed. The employee negotiated higher prices for the purchases than the current fair market prices. The employee used his influence to ensure that his employer continued doing business with the supplier and paid the inflated prices.

Red flags of the conflict scheme

- Unexplained or unusual favouritism of a particular contractor/vendor
- Business deal that is not in the best interest of the public institution
- Employee displays a keen interest in a particular vendor/contractor
- Vendor/contractor address or telephone number matches that of an employee
- Employee fails to file conflict of interest or financial disclosure forms
- Employee lives beyond his or her means or displays new wealth

Internal control red flags of conflict scheme

- Poor internal controls over purchasing
- Insufficient capacity to monitor high-risk employees or units
- Poor separation of duties in purchasing
- Poor enforcement of existing policies on conflicts of interest
- Poor documentation supporting award of contracts or subcontracts

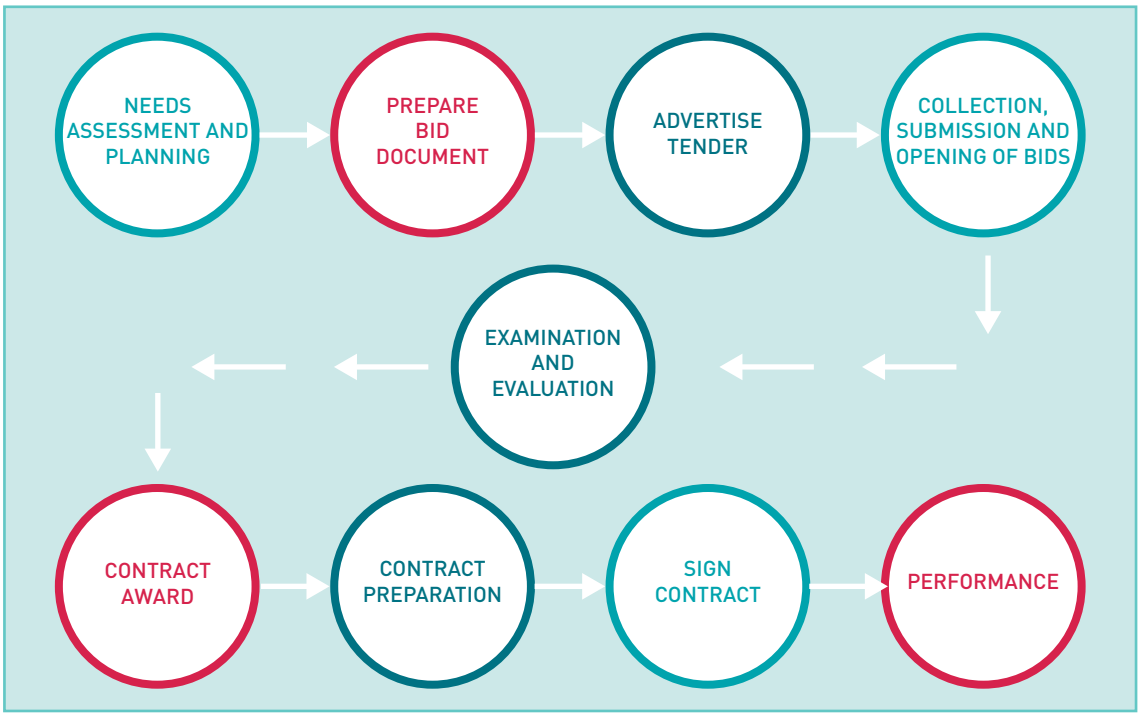
Measures for reducing vulnerability to such conflict schemes

- Establishing policies that clearly define what constitutes a conflict of interest and prohibit any such entanglements by employees of the public institution
- Establishing policies that require employees to complete an annual disclosure statement
- Establishing policies that require certain employees to provide the names and employers of immediate family members
- Educating employees about conflicts of interest
- Ensuring enforcement of existing policies on conflicts of interest
- Ensuring separation of duties in purchasing
- Ensuring full documentation supporting the award of contracts or subcontracts
- Increasing capacity to monitor high-risk employees or units
- Interviewing purchasing personnel regarding favourable treatment of one or more vendors
- Comparing the disclosed names and addresses with vendor/contractor lists

10. PROCUREMENT FRAUD AND CORRUPTION

Procurement is the process by which public organizations determine the goods and services they need to purchase and the roads, buildings and other infrastructure that must be built. The procurement process is sequential and can be divided in several different stages. The figure below breaks the process down into nine steps, beginning with the organization's determination of its needs, continuing through preparation of tender or bid documents, its advertisement if the procurement is competitive, the examination of the bids or offers submitted by companies seeking the contract, the decision to award the contract to a company or individual, the drafting and signing of the contract, and its performance.

Procurement process



10.1 BRIBES AND KICKBACKS

Corruption can occur at every stage in the process. The most common form of procurement corruption, found at every stage, is the payment of a bribe or kickback to an employee involved in the procurement decision. The payment can be made in exchange for inserting into planning documents a "need" for a good or service that a company wants to sell to the government, for drawing specifications in a way that only one firm can qualify, for ensuring the bribe-payer wins the contract, or for allowing the company that won the contract to overbill or furnish less than what the contract requires.

Bribes and kickbacks are commonly discovered when fellow employees notice that an employee is living beyond what he or she would typically be able to afford on a government salary: driving an expensive car; taking exotic, costly vacations; or sending children to school overseas.

Other signs that kickbacks may be occurring:

- *The vendor-gift bearer*. Inappropriate gifts or lavish entertainment to an employee with purchasing authority.
- *The odd couple*. A contracting officer becomes the friend of an outside supplier.
- *The too-successful bidder*. A supplier who consistently wins without any apparent competitive advantage might be providing under-the-table incentives to obtain the work.

Other methods of detection include looking for price inflation, monitoring trends in the cost of goods sold and services purchased, looking for the purchase of goods in excessive quantities or of inferior quality, conducting background checks, analysing net worth and comparing actual amounts to budgeted amounts.

10.2 MANIPULATING THE PROCESS TO FAVOUR A FIRM

There are many ways to tilt the procurement process to favour one company.

- *Limited or no advertising.* If only a few know of the bidding opportunity, competition is reduced, and the odds improve for the favoured party to win. In the extreme case, only the favoured firm is told of the opportunity.
- *Improper prequalification requirements.* Bidder competition can be further restricted by establishing improper or unnecessary prequalification requirements and then allowing only selected firms to bid. Again, prequalification, if carried out correctly, is a perfectly appropriate procedure for ensuring that bidders have the right experience and capabilities to carry out the requirements of a contract. If the standards and criteria for qualification are arbitrary or incorrect, however, they can become a mechanism for excluding competent but unwanted bidders.
- *Tailored specifications.* Persistent but unwanted parties who manage to bypass the hurdles mentioned can still be effectively eliminated by tailoring specifications to fit the favoured supplier. Using the brand name and model number of the equipment from the preferred supplier is a little too obvious, but the same results can be achieved by including specific dimensions, capacities and trivial design features that only the favoured firm can meet. The inability and failure of competitors to supply these features, which usually have no bearing on critical performance needs, are used as a ploy to reject their bids as being "non-responsive".
- *Breach of confidentiality.* Competitive bidding for contracts can work only if the bids are kept confidential until the prescribed time for determining the results. An easy way to predetermine the outcome is for the purchaser to breach the confidentiality of the bids and give the prices to the preferred supplier, who can then submit a lower figure. The mechanics are not difficult, especially if the bidders are not permitted to be present when the bids are opened.
- *Invention of new criteria.* The final opportunity to distort the outcome of competitive bidding is at the bid evaluation and comparison stage. Performed responsibly, it is an objective analysis of how each bid responds to the requirements of the bidding documents and a determination of which is the best offer. If the intention is to steer the award to a favoured bidder, the evaluation process offers almost unlimited opportunities: if necessary, and unless prevented from doing so, evaluators can invent entirely new criteria for deciding what is "best", and then apply them subjectively to get the "right" results. They are often aided in the process by issuing bidding documents that are deliberately vague and obscure about what requirements must be met and how selection decisions will be made.

10.3 TEN SIGNS OF PROCUREMENT CORRUPTION

Below are 10 simple, straightforward questions to help detect bribery, kickbacks and other forms of corruption in procurement. They can be asked about any purchase, ranging from off-the-shelf items like pencils and paper, to a new road or bridge, to the acquisition of customized information technology (IT) systems. The answers will provide a telling first indication of whether the procurement merits further scrutiny.

1. Was a cost-benefit analysis of the procurement prepared?

No individual or firm rushes out to buy a product or service without considering whether there is a need for it and whether available alternatives exist. Likewise, no government should commit public funds before determining if, on balance, the purchase is worthwhile. For every project, a cost-benefit analysis should be prepared. For simple, low-cost purchases, a short memo or spreadsheet analysis will suffice. For complex projects of high monetary value, the procuring entity should prepare a comprehensive cost-benefit analysis that considers different ways to accomplish the project's goals. If the goal is to reduce the cost of transporting goods between point A and point B, did planners analyse the cost of: *(a)* improving the existing road; *(b)* constructing a new one; or *(c)* building a rail line between the two? If the project was chosen because of corruption, it is likely that either no analysis was done, or it was an after-the-fact justification that will be easy to see through.

2. Was the purchase put out for competitive bid?

Competition is the surest way to ensure that the government gets the best product at the lowest price, and the United Nations Commission on International Trade Law Model Law on Public Procurement, the basis of virtually every national procurement statute now in force, makes competition the default option for government purchases. There will be situations when an exception is appropriate, such as a national emergency, or the existence of only one supplier who can meet the terms of reference. But any time competition is bypassed, the procurement merits heightened scrutiny.

3. How long were potential bidders given to prepare their bids?

Where the supplier is chosen by competition, the firms competing for the contract should be given sufficient time to prepare their tenders. The length will depend upon a variety of factors: the complexity of the procurement, the extent of subcontracting anticipated and the time needed for transmitting tenders. Nigerian law, for example, provides for a minimum of six weeks for large construction projects, and for World Bank-financed consultancy contracts, consulting firms must be given at least 14 days to submit an expression of interest. If the time to prepare the bid is too short, qualified firms will either decline to participate or will be unable to prepare a quality response. At the same time, the corrupt firm is likely to be given a copy of the tender long before it is made public, giving it plenty of time to develop a responsive bid.

4. Was the request for bids widely advertised?

For a competitive tender to produce the best product at the lowest price, the request for bids or tenders (the terms are frequently used interchangeably) must be widely disseminated, not just emailed to a few cronies. That will ensure all firms that might be able to meet the government's needs have a chance to respond. A notice should appear in at least one national newspaper with a large circulation, and for contracts for large public works and other purchases where foreign firms are potential suppliers, at least one major international publication as well.

5. Were the bids screened for signs of collusion?

A variety of methods are available for analysing whether the bids show signs that two or more bidders agreed with one another on the amount of the bid each would submit. A screen should be employed before the winning bidder is selected, but it can also be used afterwards and certainly should be used on large public works projects where collusion is particularly common.

6. *Did those on the committee that evaluated the bids submit a statement disclosing their financial interests?*

One way corruption can creep into the procurement process is when one or more of those evaluating the bids has a financial interest in one of the bidders. Requiring evaluators to submit a financial disclosure statement that is then verified is an important preventive measure.

7. *Who is the beneficial owner or owners of the winning bidder?*

A recent investigation in Solomon Islands revealed what is all too common in many countries: the senior civil servant responsible for approving procurement contracts secretly owned a company that was awarded a number of contracts. The firm winning the bid should be required to disclose the name of any individual who owns or controls 5 per cent or more of the firm. The disclosure should be verified.

8. *Does the request for bids allow for an audit?*

An audit, conducted before or after the contract is awarded, is a powerful tool for uncovering wrongdoing, from bid rigging through false or inflated invoices to the delivery of substandard equipment or material. Failure to include one in the bid documents and resulting contract not only makes it very difficult to investigate corruption allegations but may suggest that those preparing the bid documents or the contract are a party to corruption. The World Bank requires that contracts it finances for goods and services include a provision giving it the right to inspect bidders accounts and records and other documents relating to the bid submission and contract performance.

9. *How many technical audits will be conducted during contract implementation?*

Contracts for roads, bridges, IT systems and other purchases that require months (if not years) to complete should include mandatory audits to ensure that the work meets the contract's specifications. Once the road is built, it can be very hard to determine if the subsurface is as deep as it should be. With a technical audit an independent engineer or other professional inspects the job while it is under construction. Do the layers beneath the surface of the road contain the amount of asphalt and the size of aggregate specified in the contract? Does the IT system have the security features the contract requires to prevent hacking? A leading authority on corruption in public works, engineer A.L.M. Ameer, recommends that in construction projects, governments spend $1 for every $1,000 budgeted for construction on technical audits.

10. *Does the winning bidder have a policy against paying bribes?*

Companies should instil a sense of ethics in their employees. There is now an international standard against which to measure corporate ethics and antibribery programmes. Does the winning bidder have any such programme, and if not, why not?

11. SCREENING BIDS FOR COLLUSION

Bid screens are software programs that analyse bids received on public tenders for patterns suggesting the companies bidding colluded to rig the bid. Thanks to advances in economic theory and related developments in computer software, the use of such screens is straightforward.

Example

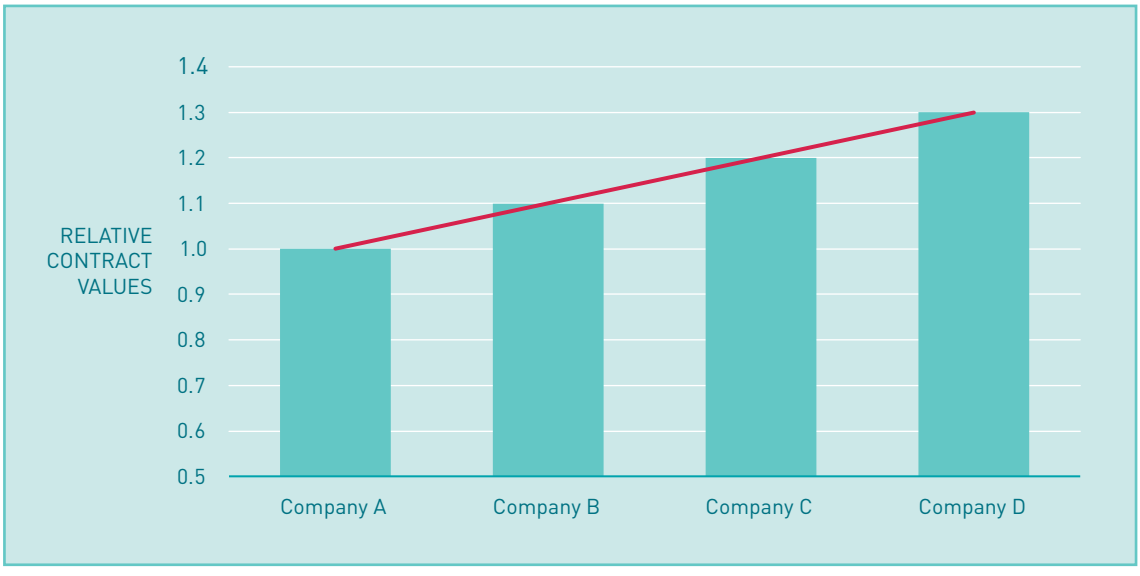
A decision has been made to construct a new road which the organization's engineers estimate will cost $57.3 million. As required by statute, the procurement organization advertises the tender and receives these four bids in response:

- Company A: $57.4 million
- Company B: $62.0 million
- Company C: $67.8 million
- Company D: $73.5 million

The bids are all from qualified companies, properly documented and responsive, and accordingly the contract is awarded to Company A. On its face, this appears to be a "clean" procurement. Now run a simple screen program.

The screen program compares each of the four bid prices to the estimated price. For each, the price the company bid is divided by the estimated price, yielding the "relative contract value". Since the Company A bid is a round number equal to the estimated price, dividing its bid price by the estimated price ($57 million/$57 million) produces 1. Because the other three companies' bids were greater than the estimate, dividing their bids by the estimated price produces relative contract values greater than 1. For Company B, it is 1.1; for Company C the number is 1.2; and for Company D, 1.3. The results are displayed in the figure below.

Suspicious bid pricing pattern



Now the procurement does not look quite so clean. The pricing pattern in fact looks quite suspicious. The bid by B is 10 per cent over the estimate, C's bid is 20 per cent over, and D's 30 per cent. What is the likelihood that this bid pattern is the result of the four companies separately and independently estimating the price at which they could build the road?

12. BREAKDOWN IN INTEGRITY PROCEDURES: A CASE STUDY

In 2009, a securities and exchange commission settled an enforcement action against a particular company.

The allegations stated that the president of the company had authorized payments to a foreign agent in order to secure certain contracts with a foreign company. The administrative order noted that the company lacked sufficient internal controls to detect or prevent such improper payments, evidenced by the president's ability to authorize large payments without meaningful underlying documentation. The initial payments were provided in the absence of a written contract. While policies in place in the company required the submission of due diligence forms prior to corporate counsel's approval when any employee wished to engage the services of a foreign agent, such forms were not submitted until five years after the initial payments. In addition, while the company's policies required contracts to include language necessitating compliance with anti-bribery laws, such language was not included in the contract until six years after the initial payments were made. Documentation by the foreign recipient company noted that the payments were for "consulting" or "marketing services" without meaningful substantiation.

LESSONS LEARNED

As this case illustrates, it is not enough to document internal controls through policies. To ensure compliance with relevant laws, the control environment must be cultivated through clearly articulated and monitored control activities that prevent management override. Furthermore, compliance with internal controls must be consistently and substantively monitored to ensure that policies and procedures are followed in all cases. Compliance professionals should be aware that creating a documented anti-corruption programme does not, by itself, create a control environment.

FRAUD INDICATORS

- Payments are authorized without requiring meaningful underlying documentation.
- Due diligence forms are not submitted in a timely manner nor reviewed.

13. TRAVEL REIMBURSEMENT FRAUD

An auditor was assigned to review the procedures governing reimbursement of personnel for travel. The review included an analysis of employee bank accounts provided for travel reimbursement, which were compared to national identity card numbers in the organization's payroll system. The comparison found 10 travel reimbursements to employees in the organization who never travel. As the audit continued, the auditor discovered that a travel office employee who recently transferred from the organization's payroll office had stolen the identity card numbers of the 10 individuals and opened bank accounts in their names. He then deposited the unauthorized travel reimbursements into these accounts.

A review of personnel with authorized access to the travel approval function disclosed that the employee submitting the fraudulent claims was given system access when he was covering for a co-worker who was on holiday. Information technology personnel did not follow internal policies and procedures and provide temporary access to the substitute employee with a five-day account expiration, even though temporary access was requested by travel management. In addition, management was not performing periodic reviews of employee travel vouchers because staff resources were limited. Because management did not follow the internal procedures, the travel embezzlement scheme was not immediately detected.

LESSONS LEARNED

Auditors should be aware of the increasing use of identity theft schemes to commit fraud. Identity theft involves the use or compromise of personally identifiable information, which includes, but is not limited to, education records, criminal and medical histories, financial transactions and any information that can be used to trace an individual's identity, such as their name, national identity card number or place of birth. Auditors should also be alert to situations where established internal controls are not functioning, such as unauthorized system access.

FRAUD INDICATORS

- The information technology department does not verify employee access restrictions.
- The information technology department does not routinely monitor access to the travel system.
- The organization does not have adequate controls to ensure that employees and management follow established policies and procedures.
- Travel and/or accounting management do not conduct periodic reviews of employee travel claims.

14. CORRUPTION AND FRAUD RISKS IN WAR ZONES

A contractor headquartered in the capital city provides services under a government contract to remote areas. Services performed in the remote areas are done pursuant to a flexibly priced contract because the costs of going to and from remote areas and delivering the services are hard to predict in advance.

While performing an assessment of the costs the contractor incurred, the auditors identified one high-risk, flexibly-priced contract in an area where insurgents were present. The contractor had subcontracted to a company familiar with the area to deliver the service. Auditors determined that the subcontract costs were 60 per cent of the contractor's total cost incurred on the contract. The auditors queried the company officials about the circumstances surrounding the subcontract award. The company officials said that the contract required the company to provide the service immediately, and the contractor sent its purchasing director to handle arrangements in the insurgency zone. However, due to the lengthy procurement process, the purchasing director decided to issue a $50,000 purchase order – the authorized signature level for his position – and then award the subcontract in accordance with the contractor's policies and procedures.

Despite some scepticism, the company officials agreed with the purchasing director's plan to initially staff the office in the area where the insurgents were operating and issue a $50,000 purchase order. The purchasing director found a subcontractor for the job. Happy to get the work, the subcontractor's president told the purchasing director that he would give the contractor a 20 per cent discount. The purchase order, intentionally silent as to the 20 per cent discount, instructed the subcontractor to submit all invoices to the contractor's headquarters in the capital. The purchasing director distributed the original purchase order to the subcontractor and forwarded a copy to the company.

The subcontractor performed on the $50,000 purchase order and submitted its first invoice to the contractor for $30,000. The subcontractor later submitted another invoice for $50,000. At the contractor's accounts payable department, the clerk observed that the subcontractor had submitted invoices totalling $80,000 on a $50,000 purchase order. Concerned about having neither a purchase order nor a subcontract for the aggregate amount invoiced, the clerk communicated with the accounts payable director, who then contacted the chief financial officer for advice.

The chief financial officer contacted the purchasing director, a long-time friend and co-worker. The purchasing director had often expressed a desire for a more lavish lifestyle for his family. The purchasing director explained that the subcontractor continued to provide the services described in the purchase order. Company officials explained to the auditors that the purchasing director did not initiate the solicitation process for awarding the subcontract as originally planned and as the contractor's policy required. The officials further explained that the purchasing director emphasized his desire to retain subcontract continuity on the contract. The officials stated that the purchasing director pleaded with the chief financial officer to modify the purchase order and pay the subcontractor's invoices as submitted. The chief financial officer agreed. He trusted his friend to make sound business decisions for the company. Afterwards, the chief financial officer advised the accounts payable director that he approved the purchase order modification practice for processing the subcontract's invoices.

As a result of the auditors' inquiries, the auditors identified another potential fraud indicator caused by the contracting officials circumventing the accounts payable and purchasing department's internal controls. Also, the auditors confirmed that the chief financial officer's purchase order modification practice and the payment of the subcontractor's invoices circumvented internal controls. In the incurred cost audit, the auditors questioned the total amounts paid to the subcontractor. The auditors questioned the subcontract costs in accordance with government procurement rules and subsequently referred the matter for investigation. The investigators found that the purchasing director received a 20 per cent discount on each of the subcontractor's invoices that the contractor paid. The purchasing director kept the cash for his personal use.

LESSONS LEARNED

Companies with employees performing in a war zone or similar environment have increased risk that assigned employees will not follow company policies and procedures. This scenario illustrates the importance of companies performing independent monitoring of employee compliance with company policies and procedures, regardless of where they perform the work. In this scenario, the accounts payable director failed to process the subcontractor's invoices in accordance with the policies, which required a review of the written subcontract agreement.

In addition, the chief financial officer facilitated the breakdown in internal controls by modifying the purchase order to match the subcontractor's invoiced amounts. The chief financial officer set the tone for the accounts payable director to circumvent the internal controls in place to ensure the proper use of federal funds and protect the contractor's assets. Early detection could have occurred had the contracting officials allowed the internal controls to function as intended. Additionally, the purchasing director openly expressing the desire to live a more lavish lifestyle is a potential fraud indicator.

This desire might have given the purchasing director the motivation to engage in the fraudulent activity. The deployment gave the purchasing director the opportunity he needed to steal government funds to live the desired lifestyle. In this scenario, the auditors were instrumental in stopping the misuse of government funds and assisting in the return of such funds to the government. The auditors recognized the fraud indicator of circumventing internal controls and referred the matter for investigation. However, including transactions initiated in the area where insurgents operated in the auditors' policy compliance audits might have aided them in identifying potential fraud indicators earlier.

FRAUD INDICATORS

- The subcontractor's 60 per cent participation in the contractor's incurred cost is a potential fraud indicator due to the significance of cost incurred.
- The purchasing director did not adhere to the contractor's purchasing policies and practices. Also, the purchasing director involved the subcontractor in the fraudulent activity by pocketing the 20 per cent discount paid to the company.
- The chief financial officer endorsed the modification of the company's purchasing policy by approving the purchase order modification process and communicating acceptance to the accounts payable director.
- The accounts payable director did not adhere to the policies and practices for processing the subcontractor's invoice for payment. The process required that the subcontractor's invoices comply with a written subcontract agreement.
- A single contracting official (purchasing director) negotiating with the subcontractor is an internal control weakness and a potential fraud indicator. The contracting officials might have known of the 20 per cent discount offered by the subcontractor if more than one contracting official had attended the negotiations with the subcontractor.
- The contractor's lack of an independent monitoring process for its employees' compliance with policies and procedures is an internal control weakness. As a result, the contractor's system of checks and balances, designed to protect its assets and detect potential fraud, failed.

Source: United States Department of Defense, *Fraud Detection Resources for Auditors,* www.dodig.mil/Resources/Fraud-Detection-Resources/.

15. MINISTRY OF DEFENCE PAYROLL AUDIT TECHNIQUES

While reviewing employee time sheets, an auditor noticed that a pharmacist was employed as both a civilian and contract employee by a unit of the Ministry of Defence. The pharmacist's independent contract authorized him to bill the organization for pharmacy services after his official workday ended and on weekends. The idea was to save the government money. Rather than hiring another full-time pharmacist, the organization's pharmacist could put in extra hours as needed and be paid as a consultant.

The auditor's review of time sheets submitted by the pharmacist disclosed the following information:

- The pharmacist was being paid for the same employee and consultant contract work hours each day. Consequently, he was being paid twice for the same work hours.
- Review of payroll records disclosed little variation in the number of contract work hours claimed, despite fluctuations in the number of overtime hours worked by other pharmacists.
- Interviews with other pharmacy employees disclosed that the suspect pharmacist's workday ended promptly at 5 p.m. and he did not work on weekends. However, the auditor's review disclosed several time sheets with charges for weekend work.
- Inquiry with management disclosed that the organization did not have policies or procedures to monitor time sheets submitted by employees who were also performing contract work.

LESSONS LEARNED

Auditors should be alert to situations where individuals are employed as both civilian and contract employees. Another common contractor payroll scheme involves contract employees not reporting to work or not working the required number of weekly or daily hours and submitting fraudulent payroll claims to the government. Whenever possible, contractor and civilian time sheets should be analysed to detect duplicate payroll claims.

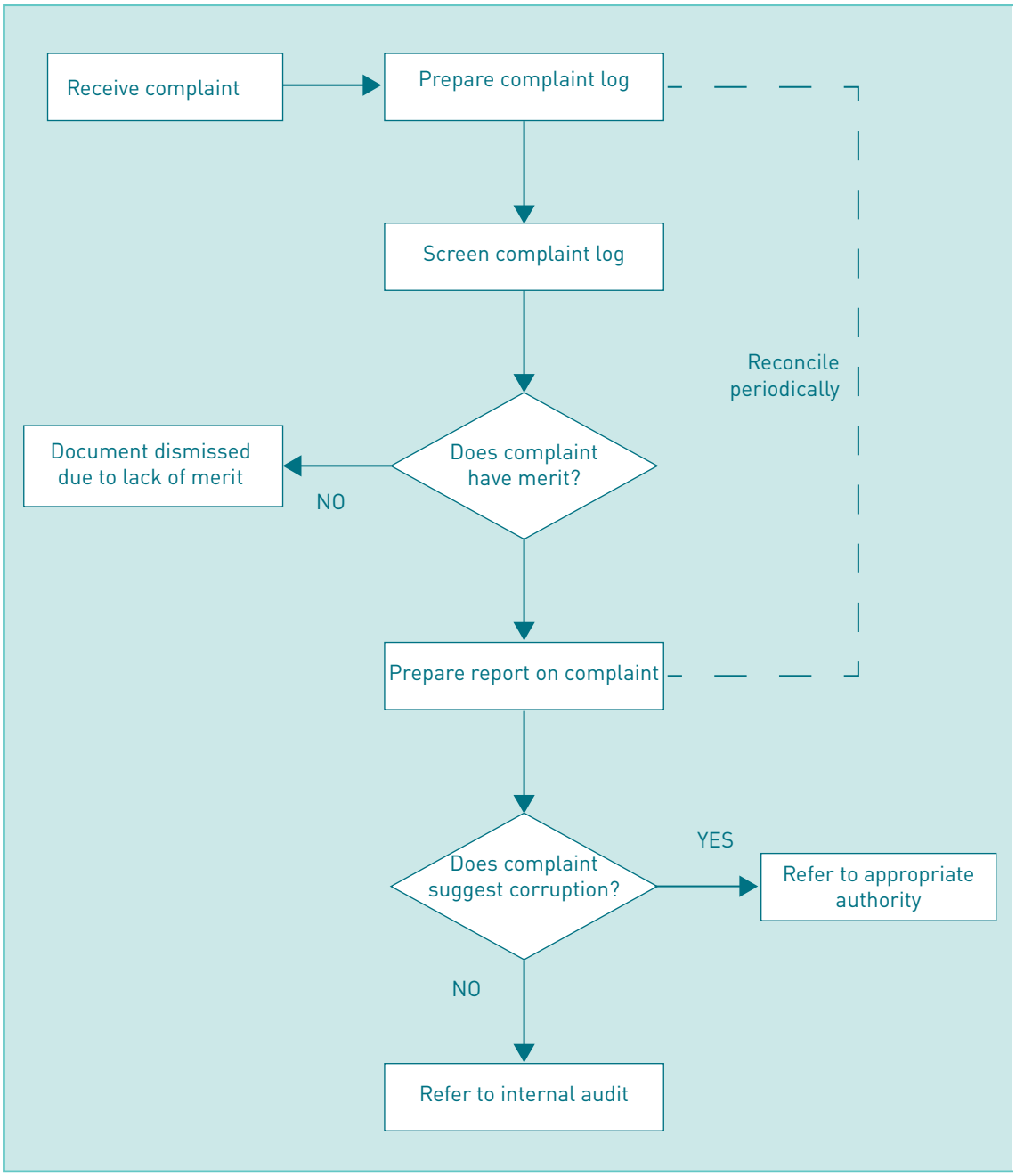
FRAUD INDICATORS

- An individual is employed as a civilian and as a contractor for the same organization.
- The employee's contract authorizes the employee to bill the government for work performed after the employee's official workday ends or on weekends.
- Analysis of contractor work hours shows little variation, despite fluctuations in overtime claims by civilians performing similar work.
- Lack of evidence to support claims for overtime work (i.e. other employees cannot verify attendance).
- Lack of policies and procedures to monitor time sheets submitted by employees who are also performing contract work.

16. SYSTEM FOR HANDLING COMPLAINTS

In addition to the model complaint handling system described in the figure below, organizations may wish to develop and implement specific whistle-blower procedures for those who identify and report alleged wrongdoing, such as those outlined in the United Nations Office on Drugs and Crime publication *Resource Guide on Good Practices in the Protection of Reporting Persons.*[1]

Model complaint handling system



[1] UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons* (2015); available at www.unodc.org/documents/corruption/Publications/2015/15-04741_Person_Guide_eBook.pdf.

17. STEPS IN REVIEWING ORGANIZATION INTEGRITY PROCEDURES/CONTROLS

1. Review any organization or government-wide ethics codes or rules that include terms of service for government employees.
2. Determine what training and materials on ethics and integrity employees are provided.
3. Discuss procedures in place with representatives of different units within the organization and at different office locations.
4. Obtain and discuss any recommendations to management submitted by internal or outside auditors relating to integrity procedures.
5. Identify management actions in response to recommendations.
6. Review record-keeping procedures.
7. Interview key personnel to gain an understanding of overall operations and the adequacy of record-keeping.
8. Obtain and review any existing key accounting policy statements or similar documentation that addresses basic accounting controls and processes.
9. Evaluate the stated policy with respect to key areas designed to ensure the adequacy of books and records, such as:
    (a) The vendor approval/contracting process (including the specific process used with respect to consultants, agents, zoning/site facilitators, public relations firms, etc.)
    (b) The vendor payment process
    (c) The petty cash process
    (d) The hiring and related payroll processes, especially with respect to "temporary" labour
10. Review the accounts payable process to ensure that proper segregation of duties and authorization requirements are in place and are being adhered to.
11. Discuss with applicable local office personnel the nature of any existing compliance function, including any internal audit group, inside legal counsel, etc.
12. Consider the impact of any existing resource constraints and their effect on the extent and nature of the capacity of the organization's personnel to comply with procedures.
13. Review general ledgers and supporting detailed accounting records, looking for unusual activity and/or suspicious vendors (e.g., large round numbers or multiple payments for the same amount). Apply Benford's Law[1] to suspicious accounts or records.
14. Review payments made to consultants and similar vendors, with particular attention paid to the purpose of the payment and the nature and extent of the service provided. Such review should include the review of large round dollar payments, offshore transfers, and unusually high expense amounts.
15. Examine expenses and reimbursements for training, travel and meals.
16. Review procedures for ensuring organizational vehicles are not employed for personal use.
17. Ensure underlying documentation exists for consultant payments, including in contracts.
18. Review payroll and perform tests to ensure that all employees exist and perform services.

[1] Benford's Law can be used to identify anomalies in data sets by reviewing the frequency with which certain values occur. Benford's Law determines that numbers in a series are not equally distributed but instead are arranged in descending frequency beginning with the number "1", which appears most frequently, then "2" and so on. When looking at a data set, an analyst can identify numbers that appear more frequently than they typically should, potentially identifying a fraudulent transaction. (For example, if a number starting with a "4" is a potential indicator of a fraudulent transaction, then there will be more transactions beginning with "4" than Benford's Law would predict.)

19. Review supporting documentation for all cash and travel advances, commissions, bonuses, wire transfers, and other cash disbursements for selected senior management personnel.
20. Review petty cash activity for unusual or unsupported payments.
21. Depending on the results of other procedures, consider performing background checks on selected vendors and consultants to identify potential associations with organization staff.
22. Review email activity and computer files of selected employees, focusing on contacts with organization vendors or bidders on procurements.

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 263-3389, www.unodc.org

V.20-02109