

INTERNATIONAL  
STANDARD

ISO  
37001

First edition  
2016-10-15

---

---

---

## Anti-bribery management systems — Requirements with guidance for use

*Systèmes de management anti-corruption — Exigences et  
recommandations de mise en oeuvre*



Reference number  
ISO 37001:2016(E)

## Contents

	Page
<b>Foreword</b>	<b>v</b>
<b>Introduction</b>	<b>vi</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Context of the organization</b>	<b>6</b>
4.1 Understanding the organization and its context	6
4.2 Understanding the needs and expectations of stakeholders	6
4.3 Determining the scope of the anti-bribery management system	6
4.4 Anti-bribery management system	7
4.5 Bribery risk assessment	7
<b>5 Leadership</b>	<b>8</b>
5.1 Leadership and commitment	8
5.1.1 Governing body	8
5.1.2 Top management	8
5.2 Anti-bribery policy	9
5.3 Organizational roles, responsibilities and authorities	9
5.3.1 Roles and responsibilities	9
5.3.2 Anti-bribery compliance function	10
5.3.3 Delegated decision-making	10
<b>6 Planning</b>	<b>10</b>
6.1 Actions to address risks and opportunities	10
6.2 Anti-bribery objectives and planning to achieve them	11
<b>7 Support</b>	<b>11</b>
7.1 Resources	11
7.2 Competence	12
7.2.1 General	12
7.2.2 Employment process	12
7.3 Awareness and training	13
7.4 Communication	13
7.5 Documented information	14
7.5.1 General	14
7.5.2 Creating and updating	14
7.5.3 Control of documented information	14
<b>8 Operation</b>	<b>15</b>
8.1 Operational planning and control	15
8.2 Due diligence	15
8.3 Financial controls	16
8.4 Non-financial controls	16
8.5 Implementation of anti-bribery controls by controlled organizations and by business associates	16
8.6 Anti-bribery commitments	17
8.7 Gifts, hospitality, donations and similar benefits	17
8.8 Managing inadequacy of anti-bribery controls	17
8.9 Raising concerns	17
8.10 Investigating and dealing with bribery	18
<b>9 Performance evaluation</b>	<b>18</b>
9.1 Monitoring, measurement, analysis and evaluation	18
9.2 Internal audit	19
9.3 Management review	20
9.3.1 Top management review	20

## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](http://www.iso.org/patents)).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

The committee responsible for this document is Project Committee ISO/PC 278, *Anti-bribery management systems*.

# Anti-bribery management systems — Requirements with guidance for use

## 1 Scope

This document specifies requirements and provides guidance for establishing, implementing, maintaining, reviewing and improving an anti-bribery management system. The system can be stand-alone or can be integrated into an overall management system. This document addresses the following in relation to the organization's activities:

- bribery in the public, private and not-for-profit sectors;
- bribery by the organization;
- bribery by the organization's personnel acting on the organization's behalf or for its benefit;
- bribery by the organization's business associates acting on the organization's behalf or for its benefit;
- bribery of the organization;
- bribery of the organization's personnel in relation to the organization's activities;
- bribery of the organization's business associates in relation to the organization's activities;
- direct and indirect bribery (e.g. a bribe offered or accepted through or by a third party).

This document is applicable only to bribery. It sets out requirements and provides guidance for a management system designed to help an organization to prevent, detect and respond to bribery and comply with anti-bribery laws and voluntary commitments applicable to its activities.

This document does not specifically address fraud, cartels and other anti-trust/competition offences, money-laundering or other activities related to corrupt practices, although an organization can choose to extend the scope of the management system to include such activities.

The requirements of this document are generic and are intended to be applicable to all organizations (or parts of an organization), regardless of type, size and nature of activity, and whether in the public, private or not-for-profit sectors. The extent of application of these requirements depends on the factors specified in [4.1](#), [4.2](#) and [4.5](#).

NOTE 1 See [Clause A.2](#) for guidance.

NOTE 2 The measures necessary to prevent, detect and mitigate the risk of bribery by the organization can be different from the measures used to prevent, detect and respond to bribery of the organization (or its personnel or business associates acting on the organization's behalf). See [A.8.4](#) for guidance.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

**3.6****top management**

person or group of people who directs and controls an *organization* (3.2) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.5) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

Note 3 to entry: Organizations can be organized depending on which legal framework they are obliged to operate under and also according to their size, sector, etc. Some organizations have both a *governing body* (3.7) and top management, while some organizations do not have responsibilities divided into several bodies. These variations, both in respect of organization and responsibilities, can be considered when applying the requirements in Clause 5.

**3.7****governing body**

group or body that has the ultimate responsibility and authority for an *organization's* (3.2) activities, governance and policies and to which *top management* (3.6) reports and by which top management is held accountable

Note 1 to entry: Not all organizations, particularly small organizations, will have a governing body separate from top management (see 3.6, Note 3 to entry).

Note 2 to entry: A governing body can include, but is not limited to, board of directors, committees of the board, supervisory board, trustees or overseers.

**3.8****anti-bribery compliance function**

person(s) with responsibility and authority for the operation of the anti-bribery *management system* (3.5)

**3.9****effectiveness**

extent to which planned activities are realized and planned results achieved

**3.10****policy**

intentions and direction of an *organization* (3.2), as formally expressed by its *top management* (3.6) or its *governing body* (3.7)

**3.11****objective**

result to be achieved

Note 1 to entry: An objective can be strategic, tactical or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, sales and marketing, procurement, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.15)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an anti-bribery objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of anti-bribery *management systems* (3.5), anti-bribery objectives are set by the *organization* (3.2), consistent with the anti-bribery *policy* (3.10), to achieve specific results.

**3.12****risk**

effect of uncertainty on *objectives* (3.11)

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

**3.20****audit**

systematic, independent and documented *process* (3.15) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.2) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

**3.21****conformity**

fulfilment of a *requirement* (3.4)

**3.22****nonconformity**

non-fulfilment of a *requirement* (3.4)

**3.23****corrective action**

action to eliminate the cause of a *nonconformity* (3.22) and to prevent recurrence

**3.24****continual improvement**

recurring activity to enhance *performance* (3.16)

**3.25****personnel**

*organization's* (3.2) directors, officers, employees, temporary staff or workers, and volunteers

Note 1 to entry: Different types of personnel pose different types and degrees of bribery *risk* (3.12) and can be treated differently by the organization's bribery risk assessment and bribery risk management procedures.

Note 2 to entry: See A.8.5 for guidance on temporary staff or workers.

**3.26****business associate**

external party with whom the *organization* (3.2) has, or plans to establish, some form of business relationship

Note 1 to entry: Business associate includes but is not limited to clients, customers, joint ventures, joint venture partners, consortium partners, outsourcing providers, contractors, consultants, sub-contractors, suppliers, vendors, advisors, agents, distributors, representatives, intermediaries and investors. This definition is deliberately broad and should be interpreted in line with the bribery *risk* (3.12) profile of the organization to apply to business associates which can reasonably expose the organization to bribery risks.

Note 2 to entry: Different types of business associate pose different types and degrees of bribery risk, and an *organization* (3.2) will have differing degrees of ability to influence different types of business associate. Different types of business associate can be treated differently by the organization's bribery risk assessment and bribery risk management procedures.

Note 3 to entry: Reference to "business" in this document can be interpreted broadly to mean those activities that are relevant to the purposes of the organization's existence.

**3.27****public official**

person holding a legislative, administrative or judicial office, whether by appointment, election or succession, or any person exercising a public function, including for a public agency or public enterprise, or any official or agent of a public domestic or international organization, or any candidate for public office

Note 1 to entry: For examples of individuals who can be considered to be public officials, see Clause A.21.

When determining this scope, the organization shall consider:

- a) the external and internal issues referred to in [4.1](#);
- b) the requirements referred to in [4.2](#);
- c) the results of the bribery risk assessment referred to in [4.5](#).

The scope shall be available as documented information.

NOTE See [Clause A.2](#) for guidance.

#### **4.4 Anti-bribery management system**

The organization shall establish, document, implement, maintain and continually review and, where necessary, improve an anti-bribery management system, including the processes needed and their interactions, in accordance with the requirements of this document.

The anti-bribery management system shall contain measures designed to identify and evaluate the risk of, and to prevent, detect and respond to, bribery.

NOTE 1 It is not possible to completely eliminate the risk of bribery, and no anti-bribery management system will be capable of preventing and detecting all bribery.

The anti-bribery management system shall be reasonable and proportionate, taking into account the factors referred to in [4.3](#).

NOTE 2 See [Clause A.3](#) for guidance.

#### **4.5 Bribery risk assessment**

**4.5.1** The organization shall undertake regular bribery risk assessment(s), which shall:

- a) identify the bribery risks the organization might reasonably anticipate, given the factors listed in [4.1](#);
- b) analyse, assess and prioritize the identified bribery risks;
- c) evaluate the suitability and effectiveness of the organization's existing controls to mitigate the assessed bribery risks.

**4.5.2** The organization shall establish criteria for evaluating its level of bribery risk, which shall take into account the organization's policies and objectives.

**4.5.3** The bribery risk assessment shall be reviewed:

- a) on a regular basis so that changes and new information can be properly assessed based on timing and frequency defined by the organization;
- b) in the event of a significant change to the structure or activities of the organization.

**4.5.4** The organization shall retain documented information that demonstrates that the bribery risk assessment has been conducted and used to design or improve the anti-bribery management system.

NOTE See [Clause A.4](#) for guidance.

even if such refusal can result in the organization losing business (except where the individual participated in the violation);

- m) at planned intervals, reporting to the governing body (if any) on the content and operation of the anti-bribery management system and of allegations of serious or systematic bribery.

NOTE See Clause A.5 for guidance.

## 5.2 Anti-bribery policy

Top management shall establish, maintain and review an anti-bribery policy that:

- a) prohibits bribery;
- b) requires compliance with anti-bribery laws that are applicable to the organization;
- c) is appropriate to the purpose of the organization;
- d) provides a framework for setting, reviewing and achieving anti-bribery objectives;
- e) includes a commitment to satisfy anti-bribery management system requirements;
- f) encourages raising concerns in good faith, or on the basis of a reasonable belief in confidence, without fear of reprisal;
- g) includes a commitment to continual improvement of the anti-bribery management system;
- h) explains the authority and independence of the anti-bribery compliance function;
- i) explains the consequences of not complying with the anti-bribery policy.

The anti-bribery policy shall:

- be available as documented information;
- be communicated in appropriate languages within the organization and to business associates who pose more than a low risk of bribery;
- be available to relevant stakeholders, as appropriate.

## 5.3 Organizational roles, responsibilities and authorities

### 5.3.1 Roles and responsibilities

Top management shall have overall responsibility for the implementation of, and compliance with, the anti-bribery management system, as described in 5.1.2.

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within and throughout every level of the organization.

Managers at every level shall be responsible for requiring that the anti-bribery management system requirements are applied and complied with in their department or function.

The governing body (if any), top management and all other personnel shall be responsible for understanding, complying with and applying the anti-bribery management system requirements, as they relate to their role in the organization.

- how to:
  - integrate and implement these actions into its anti-bribery management system processes;
  - evaluate the effectiveness of these actions.

## 6.2 Anti-bribery objectives and planning to achieve them

The organization shall establish anti-bribery management system objectives at relevant functions and levels.

The anti-bribery management system objectives shall:

- a) be consistent with the anti-bribery policy;
- b) be measurable (if practicable);
- c) take into account applicable factors referred to in 4.1, the requirements referred to in 4.2 and the bribery risks identified in 4.5;
- d) be achievable;
- e) be monitored;
- f) be communicated in accordance with 7.4;
- g) be updated as appropriate.

The organization shall retain documented information on the anti-bribery management system objectives.

When planning how to achieve its anti-bribery management system objectives, the organization shall determine:

- what will be done;
- what resources will be required;
- who will be responsible;
- when the objectives will be achieved;
- how the results will be evaluated and reported;
- who will impose sanctions or penalties.

## 7 Support

### 7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the anti-bribery management system.

**NOTE** See Clause A.7 for guidance.

- c) such personnel, top management, and the governing body (if any), file a declaration at reasonable intervals proportionate with the identified bribery risk, confirming their compliance with the anti-bribery policy.

NOTE 1 The anti-bribery compliance declaration can stand alone or be a component of a broader compliance declaration process.

NOTE 2 See [Clause A.8](#) for guidance.

### 7.3 Awareness and training

The organization shall provide adequate and appropriate anti-bribery awareness and training to personnel. Such training shall address the following issues, as appropriate, taking into account the results of the bribery risk assessment (see [4.5](#)):

- a) the organization's anti-bribery policy, procedures and anti-bribery management system, and their duty to comply;
- b) the bribery risk and the damage to them and the organization which can result from bribery;
- c) the circumstances in which bribery can occur in relation to their duties, and how to recognize these circumstances;
- d) how to recognize and respond to solicitations or offers of bribes;
- e) how they can help prevent and avoid bribery and recognize key bribery risk indicators;
- f) their contribution to the effectiveness of the anti-bribery management system, including the benefits of improved anti-bribery performance and of reporting suspected bribery;
- g) the implications and potential consequences of not conforming with the anti-bribery management system requirements;
- h) how and to whom they are able to report any concerns (see [8.9](#));
- i) information on available training and resources.

Personnel shall be provided with anti-bribery awareness and training on a regular basis (at planned intervals determined by the organization), as appropriate to their roles, the risks of bribery to which they are exposed, and any changing circumstances. The awareness and training programmes shall be periodically updated as necessary to reflect relevant new information.

Taking into account the bribery risks identified (see [4.5](#)), the organization shall also implement procedures addressing anti-bribery awareness and training for business associates acting on its behalf or for its benefit, and which could pose more than a low bribery risk to the organization. These procedures shall identify the business associates for which such awareness and training is necessary, its content, and the means by which the training shall be provided.

The organization shall retain documented information on the training procedures, the content of the training, and when and to whom it was provided.

NOTE 1 The awareness and training requirements for business associates can be communicated through contractual or similar requirements, and be implemented by the organization, the business associate or by other parties appointed for that purpose.

NOTE 2 See [Clause A.9](#) for guidance.

### 7.4 Communication

**7.4.1** The organization shall determine the internal and external communications relevant to the anti-bribery management system including:

For the control of documented information, the organization shall address the following activities, as applicable:

- distribution, access, retrieval and use;
- storage and preservation, including preservation of legibility;
- control of changes (e.g. version control);
- retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the anti-bribery management system shall be identified as appropriate, and controlled.

**NOTE** Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

## 8 Operation

### 8.1 Operational planning and control

The organization shall plan, implement, review and control the processes needed to meet requirements of the anti-bribery management system, and to implement the actions determined in 6.1, by:

- a) establishing criteria for the processes;
- b) implementing control of the processes in accordance with the criteria;
- c) keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

These processes shall include the specific controls referred to in 8.2 to 8.10.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are controlled.

**NOTE** The core text of ISO management system standards contains a requirement in relation to outsourcing, which is not used in this document, as outsourcing providers are included within the definition of business associate.

### 8.2 Due diligence

Where the organization's bribery risk assessment, as conducted in 4.5, has assessed a more than low bribery risk in relation to:

- a) specific categories of transactions, projects or activities,
- b) planned or on-going relationships with specific categories of business associates, or
- c) specific categories of personnel in certain positions (see 7.2.2.2),

the organization shall assess the nature and extent of the bribery risk in relation to specific transactions, projects, activities, business associates and personnel falling within those categories. This assessment shall include any due diligence necessary to obtain sufficient information to assess the bribery risk. The due diligence shall be updated at a defined frequency, so that changes and new information can be properly taken into account.

**NOTE 1** The organization can conclude that it is unnecessary, unreasonable or disproportionate to undertake due diligence on certain categories of personnel and business associate.

## 8.6 Anti-bribery commitments

For business associates which pose more than a low bribery risk, the organization shall implement procedures which require that, as far as practicable:

- a) business associates commit to preventing bribery by, on behalf of, or for the benefit of the business associate in connection with the relevant transaction, project, activity, or relationship;
- b) the organization is able to terminate the relationship with the business associate in the event of bribery by, on behalf of, or for the benefit of the business associate in connection with the relevant transaction, project, activity, or relationship.

Where it is not practicable to meet the requirements of a) or b) above, this shall be a factor taken into account in evaluating the bribery risk of the relationship with this business associate (see [4.5](#) and [8.2](#)) and the way in which the organization manages such risks (see [8.3](#), [8.4](#) and [8.5](#)).

NOTE See [Clause A.14](#) for guidance

## 8.7 Gifts, hospitality, donations and similar benefits

The organization shall implement procedures that are designed to prevent the offering, provision or acceptance of gifts, hospitality, donations and similar benefits where the offering, provision or acceptance is, or could reasonably be perceived as, bribery.

NOTE See [Clause A.15](#) for guidance

## 8.8 Managing inadequacy of anti-bribery controls

Where the due diligence (see [8.2](#)) conducted on a specific transaction, project, activity or relationship with a business associate establishes that the bribery risks cannot be managed by existing anti-bribery controls, and the organization cannot or does not wish to implement additional or enhanced anti-bribery controls or take other appropriate steps (such as changing the nature of the transaction, project, activity or relationship) to enable the organization to manage the relevant bribery risks, the organization shall:

- a) in the case of an existing transaction, project, activity or relationship, take steps appropriate to the bribery risks and the nature of the transaction, project, activity or relationship to terminate, discontinue, suspend or withdraw from it as soon as practicable;
- b) in the case of a proposed new transaction, project, activity or relationship, postpone or decline to continue with it.

## 8.9 Raising concerns

The organization shall implement procedures which:

- a) encourage and enable persons to report in good faith or on the basis of a reasonable belief attempted, suspected and actual bribery, or any violation of or weakness in the anti-bribery management system, to the anti-bribery compliance function or to appropriate personnel (either, directly or through an appropriate third party);
- b) except to the extent required to progress an investigation, require that the organization treats reports confidentially, so as to protect the identity of the reporter and of others involved or referenced in the report;
- c) allow anonymous reporting;
- d) prohibit retaliation, and protect those making reports from retaliation, after they have in good faith, or on the basis of a reasonable belief, raised or reported a concern about attempted, actual or suspected bribery or violation of the anti-bribery policy or the anti-bribery management system;

- f) to whom and how such information shall be reported.

The organization shall retain appropriate documented information as evidence of the methods and results.

The organization shall evaluate the anti-bribery performance and the effectiveness and efficiency of the anti-bribery management system.

NOTE See [Clause A.19](#) for guidance.

## 9.2 Internal audit

**9.2.1** The organization shall conduct internal audits at planned intervals to provide information on whether the anti-bribery management system:

- a) conforms to:
  - 1) the organization's own requirements for its anti-bribery management system;
  - 2) the requirements of this document;
- b) is effectively implemented and maintained.

NOTE 1 Guidance on auditing management systems is given in ISO 19011.

NOTE 2 The scope and scale of the organization's internal audit activities can vary depending on a variety of factors, including organization size, structure, maturity and locations.

**9.2.2** The organization shall:

- a) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits;
- b) define the audit criteria and scope for each audit;
- c) select competent auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
- d) ensure that the results of the audits are reported to relevant management, the anti-bribery compliance function, top management and, as appropriate, the governing body (if any);
- e) retain documented information as evidence of the implementation of the audit programme and the audit results.

**9.2.3** These audits shall be reasonable, proportionate and risk-based. Such audits shall consist of internal audit processes or other procedures which review procedures, controls and systems for:

- a) bribery or suspected bribery;
- b) violation of the anti-bribery policy or anti-bribery management system requirements;
- c) failure of business associates to conform to the applicable anti-bribery requirements of the organization;
- d) weaknesses in, or opportunities for improvement to, the anti-bribery management system.

**9.2.4** To ensure the objectivity and impartiality of these audit programmes, the organization shall ensure that these audits are undertaken by one of the following:

- a) an independent function or personnel established or appointed for this process; or

## 9.4 Review by anti-bribery compliance function

The anti-bribery compliance function shall assess on a continual basis whether the anti-bribery management system is:

- a) adequate to manage effectively the bribery risks faced by the organization;
- b) being effectively implemented.

The anti-bribery compliance function shall report at planned intervals, and on an *ad hoc* basis, as appropriate, to the governing body (if any) and top management, or to a suitable committee of the governing body or top management, on the adequacy and implementation of the anti-bribery management system, including the results of investigations and audits.

**NOTE 1** The frequency of such reports depends on the organization's requirements, but is recommended to be at least annually.

**NOTE 2** The organization can use a business associate to assist in the review, as long as the business associate's observations are appropriately communicated to the anti-bribery compliance function, top management and, as appropriate, the governing body (if any).

## 10 Improvement

### 10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

- a) react promptly to the nonconformity, and as applicable:
  - 1) take action to control and correct it;
  - 2) deal with the consequences;
- b) evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by:
  - 1) reviewing the nonconformity;
  - 2) determining the causes of the nonconformity;
  - 3) determining if similar nonconformities exist, or could potentially occur;
- c) implement any action needed;
- d) review the effectiveness of any corrective action taken;
- e) make changes to the anti-bribery management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

- the nature of the nonconformities and any subsequent actions taken;
- the results of any corrective action.

**NOTE** See [Clause A.20](#) for guidance.

## Annex A (informative)

### Guidance on the use of this document

#### **A.1 General**

The guidance in this annex is illustrative only. Its purpose is to indicate in some specific areas the type of actions which an organization can take in implementing its anti-bribery management system. It is not intended to be comprehensive or prescriptive, nor is an organization required to implement the following steps in order to have an anti-bribery management system that meets the requirements of this document. The steps taken by the organization should be reasonable and proportionate with regard to the nature and extent of bribery risks faced by the organization (see [4.5](#), and the factors in [4.1](#) and [4.2](#)).

Further guidance on good practice in anti-bribery management is given in the publications listed in the Bibliography.

#### **A.2 Scope of the anti-bribery management system**

##### **A.2.1 Stand-alone or integrated anti-bribery management system**

The organization can choose to implement this anti-bribery management system as a separate system, or as an integrated part of an overall compliance management system (in which case the organization can refer for guidance to ISO 19600). The organization can also choose to implement this anti-bribery management system in parallel with, or as part of, its other management systems, such as quality, environmental and information security (in which case the organization can refer to ISO 9001, ISO 14001, and ISO/IEC 27001), as well as ISO 26000 and ISO 31000.

##### **A.2.2 Facilitation and extortion payments**

**A.2.2.1** Facilitation payment is the term sometimes given to an illegal or unofficial payment made in return for services that the payer is legally entitled to receive without making such payment. It is normally a relatively minor payment made to a public official or person with a certifying function in order to secure or expedite the performance of a routine or necessary action, such as the issuing of a visa, work permit, customs clearance or installation of a telephone. Although facilitation payments are often regarded as different in nature to, for example, a bribe paid to win business, they are illegal in most locations and are treated as bribes for the purpose of this document, and they should be prohibited by the organization's anti-bribery management system.

**A.2.2.2** An extortion payment is when money is forcibly extracted from personnel by real or perceived threats to health, safety or liberty and is outside of the scope of this document. The safety and liberty of a person is paramount and many legal systems do not criminalize the making of a payment by someone who reasonably fears for their or someone else's health, safety or liberty. The organization can have a policy to permit a payment by personnel in circumstances where they have a fear of imminent danger to, their or another's health, safety or liberty.

**A.2.2.3** The organization should provide specific guidance to any personnel who can be faced with requests or demands for such payments on how to avoid them and deal with them. Such guidance could include, for example:

bribery control over its business transactions in that location than an organization which only has activities in a lower bribery risk location, where bribery is relatively rare.

- c) Although bribery risk exists in relation to many transactions or activities, the bribery risk assessment, due diligence procedures and anti-bribery controls implemented by an organization involved in a large, high value transaction or activities involving a wide range of business associates are likely to be more comprehensive than those implemented by an organization in relation to a business which involves selling small value items to multiple customers or multiple smaller transactions with a single party.
- d) An organization with a very broad range of business associates can conclude, as part of its bribery risk assessment, that certain categories of business associates, e.g. retail customers, are unlikely to pose more than a low bribery risk, and take that into account in the design and implementation of its anti-bribery management system. For example, due diligence is unlikely to be necessary, or to be a proportionate and reasonable control, in relation to retail customers who are purchasing items such as consumer goods from the organization.

**A.3.4** Although bribery risk exists in relation to many transactions, an organization should implement a more comprehensive level of anti-bribery control over a high bribery risk transaction than over a low bribery risk transaction. In this context, it is important to understand that identifying and accepting a low risk of bribery does not mean that the organization accepts the fact of bribery occurring, i.e. the risk of bribery occurring (whether a bribe might occur) is not the same as the occurrence of a bribe (the fact of the bribery itself). An organization can have a “zero tolerance” for the occurrence of bribery while still engaging in business in situations where there can be a low bribery risk, or more than a low bribery risk (as long as adequate mitigation measures are applied). Further guidance on specific controls is provided below.

## A.4 Bribery risk assessment

**A.4.1** The intention of the bribery risk assessment required by 4.5 is to enable the organization to form a solid foundation for its anti-bribery management system. This assessment identifies the bribery risks that the management system will focus on, i.e. the bribery risks deemed by the organization to be a priority for bribery risk mitigation, control implementation and allocation of anti-bribery compliance personnel, resources and activities. How the organization undertakes the bribery risk assessment, what methodology it employs, how the bribery risks are weighted and prioritized, and the level of bribery risk that is accepted (i.e. “risk appetite”) or tolerated, are all at the discretion of the organization. In particular, it is the organization that establishes its criteria for evaluating bribery risk (e.g. whether a risk is “low”, “medium” or “high”); however, in so doing, the organization should take into account its anti-bribery policy and objectives.

The following is an example of how an organization can choose to undertake this assessment.

- a) Select bribery risk evaluation criteria. For example, the organization can select three-tier criteria (e.g. “low”, “medium”, “high”), more detailed five-level or seven-level criteria, or a more detailed approach. The criteria will often take into account several factors, including the nature of the bribery risk, the likelihood of bribery occurring, and the magnitude of the consequences should it occur.
- b) Assess the bribery risks posed by the size and structure of the organization. A small organization based in one location with centralized management controls in the hands of a few people may be able to control its bribery risk more easily than a very large organization with a decentralized structure operating in many locations.
- c) Examine the locations and sectors in which the organization operates or anticipates operating, and assess the level of bribery risk these locations and sectors can pose. An appropriate bribery index can be used to assist in this assessment. Locations or sectors with a higher risk of bribery can be deemed by the organization as “medium” or “high” risk, for example, which can result in the organization imposing a higher level of controls applicable to activities by the organization in those locations or sectors.

**A.4.3** The organization can change the nature of the transaction, project, activity or relationship such that the nature and extent of the bribery risk is reduced to a level that can be adequately managed by existing, enhanced or additional anti-bribery controls.

**A.4.4** This bribery risk assessment exercise is not intended to be an extensive or overly complex exercise, and the results of the assessment will not necessarily prove to be correct (e.g. a transaction assessed as low bribery risk can turn out to have involved bribery). As far as reasonably practicable, the results of the bribery risk assessment should reflect the actual bribery risks faced by the organization. The exercise should be designed as a tool to help the organization assess and prioritize its bribery risk, and should be regularly reviewed and revised based on changes in the organization or circumstances (e.g. new markets or products, legal requirements, experiences gained).

NOTE Further guidance is given in ISO 31000.

## A.5 Roles and responsibilities of governing body and top management

**A.5.1** Many organizations have some form of governing body (e.g. a board of directors or supervisory board) that has general oversight responsibilities with respect to the organization. These responsibilities include oversight regarding the organization's anti-bribery management system. However, the governing body generally does not exercise day-to-day direction over the activities of the organization. That is the role of executive management (e.g. the chief executive officer, chief operating officer), which is referred to in this document as "top management". With respect to the anti-bribery management system, the governing body should be knowledgeable about the content and operation of the management system, and should exercise reasonable oversight with respect to the adequacy, effectiveness and implementation of the management system. It should regularly receive information regarding the performance of the management system through the management review process (this might be to the entire governing body, or to a committee of the body, such as the audit committee). In this respect, the anti-bribery compliance function should be able to report information about the management system directly to the governing body (or the appropriate committee thereof).

**A.5.2** Some organizations, particularly smaller ones, might not have a separate governing body, or the roles of the governing body and executive management might be combined in one group or even one individual. In such cases, the group or individual will have the responsibilities allocated in this document to top management and the governing body.

NOTE Leadership commitment is sometimes referred to as "tone at the top" or "tone from the top".

## A.6 Anti-bribery compliance function

**A.6.1** The number of people working in the anti-bribery compliance function depends on factors such as the size of the organization, the extent of bribery risk the organization faces, and the resultant work load of the function. In a small organization, the anti-bribery compliance function is likely to be one person who is assigned the responsibility on a part-time basis, and who combines this responsibility with other responsibilities. Where the extent of bribery risk and resultant work load justifies it, the anti-bribery compliance function can be one person who is assigned the responsibility on a full-time basis. In large organizations, the function is likely to be staffed by several people. Some organizations can assign responsibility to a committee that embodies a range of relevant expertise. Some organizations can choose to use a third party to undertake some or all of the anti-bribery compliance function, and this is acceptable provided that an appropriate manager within the organization retains overall responsibility for and authority over the anti-bribery compliance function and supervises the services provided by the third party.

**A.6.2** This document requires that the anti-bribery compliance function be staffed by person(s) who have the appropriate competence, status, authority and independence. In this respect:

## A.8 Employment procedures

### A.8.1 Due diligence on personnel

When undertaking due diligence on persons prior to appointing them as personnel, the organization, depending on the persons' proposed functions and corresponding bribery risk, can take actions such as:

- a) discussing the organization's anti-bribery policy with prospective personnel at interview, and forming a view as to whether they appear to understand and accept the importance of compliance;
- b) taking reasonable steps to verify that prospective personnel's qualifications are accurate;
- c) taking reasonable steps to obtain satisfactory references from prospective personnel's previous employers;
- d) taking reasonable steps to determine whether prospective personnel have been involved in bribery;
- e) taking reasonable steps to verify that the organization is not offering employment to prospective personnel in return for their having, in previous employment, improperly favoured the organization;
- f) verifying that the purpose of offering employment to prospective personnel is not to secure improper favourable treatment for the organization;
- g) taking reasonable steps to identify the prospective personnel's relationship to public officials.

### A.8.2 Performance bonuses

Arrangements for compensation, including bonuses and incentives, can encourage, even unintentionally, personnel to participate in bribery. For example, if a manager receives a bonus based on the award of a contract to the organization, the manager could be tempted to pay a bribe, or to turn a blind eye to an agent or joint venture partner paying a bribe, so as to secure the award of the contract. The same outcome could occur if too much pressure is put on a manager to perform (e.g. if the manager could be dismissed for failing to achieve over-ambitious sales targets). The organization needs to pay careful attention to these aspects of compensation to ensure as far as reasonable that they do not act as bribery incentives.

Personnel evaluations, promotions, bonuses and other rewards could be used as incentives for personnel to perform in accordance with the organization's anti-bribery policy and anti-bribery management system. However, the organization needs to be cautious in this case, as the threat of loss of bonus, etc. can result in personnel concealing failures in the anti-bribery management system.

Personnel should be made aware that violating the anti-bribery management system so as to improve their performance rating in other areas (e.g. achieving a sales target) is not acceptable and should result in corrective and/or disciplinary action.

### A.8.3 Conflicts of interest

The organization should identify and evaluate the risk of internal and external conflicts of interest. The organization should clearly inform all personnel of their duty to report any actual or potential conflict of interest such as family, financial or other connection directly or indirectly related to their line of work. This helps an organization to identify situations where personnel may facilitate or fail to prevent or report bribery, e.g.

- a) when the organization's sales manager is related to a customer's procurement manager, or
- b) when an organization's line manager has a personal financial interest in a competitor's business.

The organization should preferably keep a record of any circumstances of actual or potential conflicts of interest and whether actions were taken to mitigate the conflict.

by those temporary staff or workers (if any) is adequately dealt with by treating the temporary staff or workers as its own personnel for training and control purposes, or whether to impose appropriate controls through the business associate which provides the temporary staff or workers.

## A.9 Awareness and training

**A.9.1** The intention of the training is to help ensure that relevant personnel understand, as appropriate to their role in or with the organization, the following:

- a) the bribery risks they and their organization face;
- b) the anti-bribery policy;
- c) the aspects of the anti-bribery management system relevant to their role;
- d) any necessary preventive and reporting actions they need to take in relation to any bribery risk or suspected bribery.

**A.9.2** The formality and extent of the training depends on the size of the organization and the bribery risks faced. It could be conducted as an online module, or by in-person methods (e.g. classroom sessions, workshops, roundtable discussions between relevant personnel, or by one-to-one sessions). The method of the training is less important than the outcome, which is that all relevant personnel should understand the issues referred to in [A.9.1](#).

**A.9.3** In-person training is recommended for the governing body (if any), and any personnel (irrespective of their positions or hierarchy within the organization) and business associates who are involved in operations and processes with more than a low bribery risk.

**A.9.4** If the relevant person(s) assigned the anti-bribery compliance function does not have sufficient related experience, the organization should provide any training necessary for him or her to perform the anti-bribery compliance function adequately.

**A.9.5** The training can take place as stand-alone anti-bribery training, or can be part of the organization's overall compliance and ethics training or induction programme.

**A.9.6** The content of the training can be adapted to the role of the personnel. Personnel who do not face any significant bribery risk in their role could receive very simple training on the organization's policy, so that they understand the policy, and know what to do if they see a potential violation. Personnel whose role involves a high bribery risk should receive more detailed training.

**A.9.7** The training should be repeated as often as necessary so that personnel are up to date with the organization's policies and procedures, any developments in relation to their role, and any regulatory changes.

**A.9.8** Applying the training and awareness requirements to business associates identified under the requirements of [7.3](#) poses particular challenges because the employees of such business associates generally do not work directly for the organization, and the organization typically will not have direct access to such employees for purposes of training. The actual training of employees working for business associates will normally be conducted by the business associates or by other parties retained for that purpose. It is important that employees who work for business associates who could pose more than a low bribery risk to the organization are aware of the issue and receive training reasonably intended to reduce this risk. The content of [7.3](#) requires that the organization, at a minimum, identify the business associates whose employees should be provided anti-bribery training, what the minimum content of such training should be, and that such training should be conducted. The training itself may be provided by the business associate, by designated other parties or, if the organization so chooses, by the organization.

- iii) have any direct or indirect links to the organization's customer or client or to a relevant public official which could lead to bribery (this would include persons who are not public officials themselves, but who may be directly or indirectly related to public officials, candidates for public office, etc.);
- 6) the structure of the transaction and payment arrangements;
- b) the nature, type and extent of due diligence undertaken will depend on factors such as the ability of the organization to obtain sufficient information, the cost of obtaining information, and the extent of the possible bribery risk posed by the relationship;
- c) the due diligence procedures implemented by the organization on its business associates should be consistent across similar bribery risk levels (high bribery risk business associates in locations or markets where there is a high risk of bribery are likely to require a significantly higher level of due diligence than lower bribery risk business associates in low bribery risk locations or markets);
- d) different types of business associates are likely to require different levels of due diligence, for example:
  - 1) from the perspective of the organization's potential legal and financial liability, business associates pose a higher bribery risk to the organization when they are acting on the organization's behalf or for its benefit than when they are providing products or services to the organization. For example, an agent involved in assisting an organization to obtain a contract award could pay a bribe to a manager of the organization's customer to help the organization win the contract, and so could result in the organization being responsible for the agent's corrupt conduct. As a result, the organization's due diligence on the agent is likely to be as comprehensive as possible. On the other hand, a supplier selling equipment or material to the organization and which has no involvement with the organization's customers or public officials that are relevant to the organization's activities is less likely to be able to pay a bribe on the organization's behalf or for its benefit, and so the level of due diligence on the supplier could be lower;
  - 2) the level of influence which the organization has over its business associates also affects the organization's ability to obtain information directly from those business associates as part of its due diligence. It may be relatively easy for an organization to require its agents and joint venture partners to provide extensive information about themselves as part of a due diligence exercise prior to the organization committing to work with them, as the organization has a degree of choice over with whom it contracts in this situation. However, it may be more difficult for an organization to require a customer or client to provide information about themselves or to fill in due diligence questionnaires. This could be because the organization would not have sufficient influence over the client or customer to be able to do so (for example where the organization is involved in a competitive tender to provide services to the customer);
- e) the due diligence undertaken by the organization on its business associates may include, for example:
  - 1) a questionnaire sent to the business associate in which it is asked to answer the questions referred to in A.10.3 a);
  - 2) a web-search on the business associate and its shareholders and top management to identify any bribery-related information;
  - 3) searching appropriate government, judicial and international resources for relevant information;
  - 4) checking publicly available debarment lists of organizations that are restricted or prohibited from contracting with public or government entities kept by national or local governments or multilateral institutions, such as the World Bank;
  - 5) making enquiries of appropriate other parties about the business associate's ethical reputation;

- b) assessing:
  - 1) the necessity and legitimacy of the services to be provided by a business associate (excluding clients or customers) to the organization;
  - 2) whether the services were properly carried out;
  - 3) whether any payments to be made to the business associate are reasonable and proportionate with regard to those services. This is particularly important in order to avoid the risk that the business associate uses part of the payment made to it by the organization to pay a bribe on behalf of or for the benefit of the organization. For example, if an agent has been appointed by the organization to assist with sales and is to be paid a commission or a contingency fee on award of a contract to the organization, the organization needs to be reasonably satisfied that the commission payment is reasonable and proportionate with regard to the legitimate services actually carried out by the agent, taking into account the risk assumed by the agent in case the contract is not awarded. If a disproportionately large commission or contingency fee is paid, there is an increased risk that part of it could be improperly used by the agent to induce a public official or an employee of the organization's client to award the contract to the organization. The organization may also request that its business associates provide documentation that demonstrates that the services have been provided;
- c) awarding contracts, where possible and reasonable, only after a fair and, where appropriate, transparent competitive tender process between at least three competitors has taken place;
- d) requiring at least two persons to evaluate the tenders and approve the award of a contract;
- e) implementing a separation of duties, so that personnel who approve the placement of a contract are different from those requesting the placement of the contract and are from a different department or function from those who manage the contract or approve work done under the contract;
- f) requiring the signatures of at least two persons on contracts, and on documents which change the terms of a contract or which approve work undertaken or supplies provided under the contract;
- g) placing a higher level of management oversight on potentially high bribery risk transactions;
- h) protecting the integrity of tenders and other price-sensitive information by restricting access to appropriate people;
- i) providing appropriate tools and templates to assist personnel (e.g. practical guidance, do's and don'ts, approval ladders, checklists, forms, IT workflows).

NOTE Further examples of controls and guidance are given in ISO 19600.

## A.13 Implementation of the anti-bribery management system by controlled organizations and by business associates

### A.13.1 General

**A.13.1.1** The reason for the requirement in 8.5 is that both controlled organizations and business associates can pose a bribery risk to the organization. The types of bribery risk which the organization is aiming to avoid in these cases are, for example:

- a) a subsidiary of the organization paying a bribe with the result that the organization can be liable;
- b) a joint venture or joint venture partner paying a bribe to win work for a joint venture in which the organization participates;
- c) a procurement manager of a customer or client demanding a bribe from the organization in return for a contract award;

- a) The organization determines whether the business associate has in place appropriate anti-bribery controls which manage the relevant bribery risk. The organization should make this determination after undertaking appropriate due diligence (see Clause A.10). The organization is trying to verify that these controls manage the bribery risk relevant to the transaction between the organization and the business associate. The organization does not need to verify that the business associate has controls over its wider bribery risks. Note that both the extent of the controls and the steps that the organization needs to take to verify these controls should be reasonable and proportionate to, the relevant bribery risk. If the organization has determined as far as it reasonably can that the business associate does have in place appropriate controls, the requirement of 8.5 is addressed in relation to that business associate. See A.13.3.4 for comments on appropriate types of controls.
- b) If the organization identifies that the business associate does not have in place appropriate anti-bribery controls that manage the relevant bribery risks, or if it is not possible to verify whether it has these controls in place, the organization undertakes the following further steps.
  - 1) If it is practicable (see A.13.3.3) to do so, the organization requires the business associate to implement anti-bribery controls (see A.13.3.4) in relation to the relevant transaction, project or activity.
  - 2) Where it is not practicable (see A.13.3.3) to require the business associate to implement anti-bribery controls, the organization takes this factor into account when assessing the bribery risks that the business associate poses, and the way in which the organization manages such risks. This does not mean that the organization cannot go ahead with the relationship or transaction. However, the organization should consider, as part of the bribery risk assessment, the likelihood of the business associate being involved in bribery, and the organization should take the absence of such controls into account in assessing the overall bribery risk. If the organization believes that the bribery risks posed by this business associate are unacceptably high, and the bribery risk cannot be reduced by other means (e.g. re-structuring the transaction), the provisions of 8.8 will apply.

**A.13.3.3** Whether or not it is practicable for the organization to require a non-controlled business associate to implement controls depends on the circumstances. For example:

- a) It will normally be practicable when the organization has a significant degree of influence over the business associate. For example, where the organization is appointing an agent to act on its behalf in a transaction, or is appointing a sub-contractor with a large scope of work. In this case, the organization will normally be able to make implementation of anti-bribery controls a condition of appointment.
- b) It will normally not be practicable when the organization does not have a significant degree of influence over the business associate, e.g.
  - 1) a client for a project;
  - 2) a specific sub-contractor or supplier nominated by the client;
  - 3) a major sub-contractor or supplier when the bargaining power of the supplier or sub-contractor is far greater than that of the organization (e.g. when the organization is buying components from a major supplier on the supplier's standard terms).
- c) It will normally not be practicable when the business associate lacks the resources or expertise to be able to implement controls.

**A.13.3.4** The types of controls required by the organization depend on the circumstances. They should be reasonable and proportionate to the bribery risk, and at a minimum should include the relevant bribery risk within their scope. Depending on the nature of the business associate and the nature of the bribery risk it poses, the organization may, for example, take the following steps.

**A.14.3** In the case of a business associate which poses a more than low bribery risk, the organization should, where practicable, obtain anti-bribery commitments from that business associate.

- a) It will normally be practicable to require these commitments when the organization has influence over the business associate and it can insist on the business associate giving these commitments. The organization is likely to be able to require these commitments, for example, where the organization is appointing an agent to act on its behalf in a transaction, or is appointing a subcontractor with a large scope of work.
- b) The organization may not have sufficient influence to be able to require these commitments in relation to, for example, dealings with major customers or clients, or when the organization is buying components from a major supplier on the supplier's standard terms. In these cases, the absence of such provisions does not mean that the project or relationship should not go ahead, but the absence of such commitment should be regarded as a relevant factor in the bribery risk assessment and due diligence undertaken under 4.5 and 8.2.

**A.14.4** These commitments should as far as possible be obtained in writing. This could be as a separate commitment document, or as part of a contract between the organization and the business associate.

## **A.15 Gifts, hospitality, donations and similar benefits**

**A.15.1** The organization needs to be aware that gifts, hospitality, donations and other benefits can be perceived by a third party (e.g. a business competitor, the press, a prosecutor, or judge), to be for the purpose of bribery even if neither the giver nor the receiver intended it to be for this purpose. A useful control mechanism is to avoid as far as possible any gifts, hospitality, donations and other benefits which could reasonably be perceived by a third party to be for the purpose of bribery.

**A.15.2** The benefits referred to in 8.7 could include, for example:

- a) gifts, entertainment and hospitality;
- b) political or charitable donations;
- c) client representative or public official travel;
- d) promotional expenses;
- e) sponsorship;
- f) community benefits;
- g) training;
- h) club memberships;
- i) personal favours;
- j) confidential and privileged information.

**A.15.3** In relation to gifts and hospitality, the procedures implemented by the organization could, for example, be designed to:

- a) control the extent and frequency of gifts and hospitality by:
  - 1) a total prohibition on all gifts and hospitality; or
  - 2) permitting gifts and hospitality, but limiting them by reference to such factors as:
    - i) a maximum expenditure (which may vary according to the location and the type of gift and hospitality);

- g) prohibit paying the expenses of family members or friends;
- h) prohibit the paying of holiday or recreational expenses.

## A.16 Internal audit

**A.16.1** The requirement in 9.2 does not mean that an organization is obliged to have its own separate internal audit function. It requires the organization to appoint a suitable, competent and independent function or person with responsibility to undertake this audit. An organization may use a third party to operate its entire internal audit program, or may engage a third party to implement certain portions of an existing program.

**A.16.2** The frequency of audit will depend on the organization's requirements. It is likely that some sample projects, contracts, procedures, controls and systems will be selected for audit each year.

**A.16.3** The selection of the sample can be risk-based, so that, for example, a high bribery risk project would be selected for audit in priority to a low bribery risk project.

**A.16.4** The audits will normally need to be planned in advance so that the relevant parties have the necessary documents and time available. However, in some cases, the organization may find it useful to implement an audit which the parties being audited do not expect.

**A.16.5** If an organization has a governing body, the governing body may also direct the organization's selection and frequency of audits as it deems necessary, in order to exercise independence and help ensure audits are targeted at the organization's primary bribery risk areas. The governing body may also require access to all audit reports and results, and that any audits identifying certain types of higher bribery risk issues or bribery risk-indicators be reported to the governing body when the audit has been completed.

**A.16.6** The intention of the audit is to provide reasonable assurance to the governing body (if any) and top management that the anti-bribery management system has been implemented and is operating effectively, to help prevent and detect bribery, and to provide a deterrent to any potentially corrupt personnel (as they will be aware that their project or department could be selected for audit).

## A.17 Documented information

The documented information under 7.5.1 may include:

- a) receipt of anti-bribery policy by personnel;
- b) provision of anti-bribery policy to business associates who pose more than a low risk of bribery;
- c) the policies, procedures and controls of the anti-bribery management system;
- d) bribery risk assessment results (see 4.5);
- e) anti-bribery training provided (see 7.3);
- f) due diligence carried out (see 8.2);
- g) the measures taken to implement the anti-bribery management system;
- h) approvals and records of gifts, hospitality, donations and similar benefits given and received (see 8.7);

**A.18.6** In undertaking the investigation and any follow up action, the organization needs to consider relevant factors, for example:

- a) applicable laws (legal advice may need to be taken);
- b) the safety of personnel;
- c) the risk of defamation when making statements;
- d) the protection of people making reports and of others involved or referenced in the report (see [8.9](#));
- e) potential criminal, civil and administrative liability, financial loss and reputational damage for the organization and individuals;
- f) any legal obligation, or benefit to the organization, to report to the authorities;
- g) keeping the issue and investigation confidential until the facts have been established;
- h) the need for top management to require the full co-operation of personnel in the investigation.

**A.18.7** The results of the investigation should be reported to top management or the compliance function as appropriate. If the results are reported to top management, they should also be communicated to the anti-bribery compliance function.

**A.18.8** Once the organization has completed its investigation, and/or has sufficient information to be able to make a decision, the organization should implement appropriate follow up actions. Depending on the circumstances and the severity of the issue, these could include one or more of the following:

- a) terminating, withdrawing from, or modifying the organization's involvement in, a project, transaction or contract;
- b) repaying or reclaiming any improper benefit obtained;
- c) disciplining responsible personnel (which, depending on the severity of the issue, could range from, a warning for a minor offence to dismissal for a serious offence);
- d) reporting the matter to the authorities;
- e) if bribery has occurred, taking action to avoid or deal with any possible consequent legal offences (e.g. false accounting which may occur where a bribe is falsely described in the accounts, a tax offence where a bribe is wrongly deducted from income, or money-laundering where the proceeds of a crime are dealt with).

**A.18.9** The organization should review its anti-bribery procedures to examine whether the issue arose because of some inadequacy in its procedures and, if so, it should take immediate and appropriate steps to improve its procedures.

## A.19 Monitoring

Monitoring of the anti-bribery management system may include, for example, the following areas:

- a) effectiveness of training;
- b) effectiveness of controls, for example by sample testing outputs;
- c) effectiveness of allocation of responsibilities for meeting anti-bribery management system requirements;
- d) effectiveness in addressing compliance failures previously identified;
- e) instances where internal audits are not performed as scheduled.

- b) officials of political parties;
- c) candidates for public office;
- d) government employees, including employees of ministries, government agencies, administrative tribunals and public boards;
- e) officials of public international organizations, e.g. the World Bank, the United Nations, the International Monetary Fund;
- f) employees of state-owned enterprises, unless the enterprise operates on a normal commercial basis in the relevant market, i.e. on a basis which is substantially equivalent to that of a private enterprise, without preferential subsidies or other privileges (see Reference [17]).

In many jurisdictions, relatives and close associates of public officials are also considered to be public officials for the purpose of anti-corruption laws.

## A.22 Anti-bribery initiatives

Although not a requirement of this document, the organization may find it useful to participate in, or take account of the recommendations of, any sectoral or other anti-bribery initiatives which promote or publish good anti-bribery practice relevant to the organization's activities.

- [25] International Corporate Governance Network, ICGN Statement and Guidance on Anti-Corruption Practices, London, 2009
- [26] World Economic Forum, Partnering Against Corruption Principles for Countering Bribery, An Initiative of the World Economic Forum in Partnership with Transparency International and the Basel Institute on Governance, Geneva
- [27] Committee of the Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework, May 2013