ISO/PC **278** Secretariat: **BSI**

Voting begins on:
2016-01-05

Voting terminates on:
2016-04-05

Anti-bribery management systems

Systèmes de management anti-corruption

ICS: 03.100.01

Reference number
ISO/DIS 37001:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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).

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).

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information. The committee responsible for this document is Technical Committee ISO/TC 207, Environmental management, Subcommittee SC 1, Environmental management systems.

ISO 37001 was prepared by Technical Committee ISO/TC 278, *Anti-bribery management systems*.

NOTE TO THIS TEXT (which will not be included in the published International Standard):

This text has been prepared using the a high level structure, identical core text, and common terms with core definitions, designed to benefit users implementing multiple ISO management system standards, as set out in Annex SL, Appendix 2 of the ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2015.
The text of Annex SL is shown in the main body of the text (Clauses 1 to 10) by the use of blue font. All other text is shown in black font. This is only to facilitate analysis and will not be incorporated in the final version of ISO 37001.

Introduction

Bribery is a widespread phenomenon. It raises serious moral, economic and political concerns, undermines good governance, hinders development and distorts competition. It erodes justice, undermines human rights and is an obstacle to the relief of poverty. It also increases the cost of doing business, introduces uncertainties into commercial transactions, increases the cost of goods and services, diminishes the quality of products and services, which may lead to loss of life and property, destroys trust in institutions and interferes with the fair and efficient operation of markets.

Governments have made progress in addressing bribery through international agreements such as the Organization for Economic Co-operation and Development's Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and the United Nations Convention against Corruption and through their national laws. In most jurisdictions, it is an offence for individuals to engage in bribery and there is a growing trend to make organizations as well as individuals liable for bribery.

Nevertheless, the law alone is not sufficient to solve this problem.

Organizations therefore have a responsibility to proactively contribute to combating bribery. This can be achieved through leadership commitment to establishing a culture of integrity, transparency, openness and compliance. The nature of an organization's culture is critical to the success or failure of an anti-bribery management system.

This International Standard is intended to support the establishment of such a culture by providing an anti-bribery management system framework.

A well-managed organization should have a compliance policy supported by appropriate management systems to assist it in complying with its legal obligations and commitment to integrity. An anti-bribery policy is a component of an overall compliance policy. The anti-bribery policy and supporting management system helps an organization to avoid or mitigate the costs, risks and damage of involvement in bribery, to promote trust and confidence in business dealings and to enhance its reputation.

This International Standard reflects international good practice and is applicable across all jurisdictions. It is applicable to small, medium and large organizations in all sectors, including public, private and not-for-profit sectors. The bribery risks facing an organization vary according to factors such as the size of the organization, the locations and sectors in which the organization operates and the nature, scale and complexity of the organization's activities. Therefore, this International Standard specifies the implementation by the organization of policies, procedures and controls which are reasonable and proportionate according to the bribery risks the organization faces. Annex A provides guidance on implementing the requirements of this International Standard.

Conformity with this International Standard cannot provide assurance that no bribery has occurred or will take place in relation to the organization as it is not possible to completely eliminate the risk of bribery. However, this International Standard can help the organization implement reasonable and proportionate measures designed to prevent, detect and address bribery.

This International Standard can be used in conjunction with ISO 19600 and other management system standards such as ISO 9001, ISO 14001, ISO 22000, as well as ISO 26000 and ISO 31000.

1 Scope

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

a) bribery in the public, private and not-for-profit sectors;

b) bribery by the organization;

c) bribery by the organization's personnel acting on the organization's behalf or for its benefit;

d) bribery by the organization's business associates acting on the organization's behalf or for its benefit;

e) bribery of the organization;

f) bribery of the organization's personnel in relation to the organization’s activities;

g) bribery of the organization's business associates in relation to the organization’s activities;

h) direct and indirect bribery (e.g. a bribe offered or accepted through or by a third party).

This International Standard 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 address bribery and comply with anti-bribery laws and voluntary commitments applicable to its activities.

In this International Standard, the term "bribery" is used to refer to the offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person's duties.

Moreover, this general use of the term “bribery” will be further informed by the anti-bribery laws applicable to the organization and an anti-bribery management system designed to help the organization.

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

The requirements of this International Standard 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.

If the whole or part of any requirement in this International Standard is in conflict with, or prohibited by, any applicable law, then the organization will not be obliged to conform with the relevant whole or part of that requirement.

NOTE 1 See A.2 for guidance.

NOTE 2 The measures necessary to prevent, detect and address the risk of bribery by the organization may be different from the measures used to prevent, detect and address 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

3 Terms and definitions

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

3.01
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.10)

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: For organizations with more than one operating unit, a single operating unit may be defined as an organization.

3.02
stakeholder
person or *organization* (3.01) that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: A stakeholder can be internal or external to the organization.

3.03
requirement
need that is stated and obligatory

3.04
management system
set of interrelated or interacting elements of an *organization* (3.01) to establish *policies* (3.09) and *objectives* (3.10) and *processes* (3.14) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

3.05
top management
person or group of people who directs and controls an *organization* (3.01) 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* (3.04) 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 may have both a *governing body* (3.06) and *top management* (3.05), while some organizations may 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.

3.06
governing body
group or body that has the ultimate responsibility and authority for an *organization's* (3.01) activities, governance and policies and to which *top management* (3.05) reports and is held accountable.

EXAMPLE Board of directors, supervisory board, trustees or overseers.

3.07
anti-bribery compliance function
person(s) with responsibility and authority for the operation of the anti-bribery *management system* (3.04)

3.08
effectiveness
extent to which planned activities are realized and planned results achieved

3.09
policy
intentions and direction of an *organization* (3.01), as formally expressed by its *top management* (3.05) or its *governing body* (3.06)

3.10
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* (3.14)).

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, anti-bribery objectives are set by the organization, consistent with the anti-bribery policy, to achieve specific results.

3.11
risk
effect of uncertainty on *objectives* (3.10)

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

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

3.12
competence
ability to apply knowledge and skills to achieve intended results

3.13
documented information
information required to be controlled and maintained by an *organization* (3.01) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.04), including related *processes* (3.14);

— information created in order for the organization to operate (documentation);

3.14
process
set of interrelated or interacting activities which transforms inputs into outputs

3.15
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.14), products (including services), systems or *organizations* (3.01).

3.17
monitoring
determining the status of a system, a *process* (3.14) or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

3.18
measurement
process (3.14) to determine a value

3.19
audit
systematic, independent and documented *process* (3.14) 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 itself, or by an external party on its behalf.

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

3.20
conformity
fulfilment of a *requirement* (3.03)

3.21
nonconformity
non-fulfilment of a *requirement* (3.03)

3.22
corrective action
action to eliminate the cause of a *nonconformity* (3.21) and to prevent recurrence

3.23
continual improvement
recurring activity to enhance *performance* (3.15)

Note 1 to entry: See 10.2.

3.24
personnel
organization's (3.01) directors, officers, employees, temporary staff or workers, and volunteers

Note 1 to entry: See A.8.5 for guidance on temporary staff or workers.

Note 2 to entry: Different types of personnel pose different types and degrees of bribery *risk* (3.11) and therefore may

business associate
external party with whom the *organization* (3.01) 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 profile of the organization to apply to business associates which may reasonably expose the organization to bribery risks.

Note 2 to entry: Different types of business associate pose different types and degrees of bribery *risk* (3.11), and an *organization* (3.01) will have differing degrees of ability to influence different types of business associate. Different types of business associate may therefore be treated differently by the organization's bribery risk assessment and bribery risk management procedures.

Note 3 to entry: Reference to “business” in this International Standard can be interpreted broadly to mean those activities that are relevant to the purposes of the organization’s existence.

3.26
public official
any person holding a legislative, administrative or judicial office, whether appointed or elected, 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

Note 1 to entry: For examples of individuals who can be considered to be public officials, see A.20.

3.27
third party
person or body that is independent of the organization

3.28
conflict of interest
situation where business, financial, family, political or personal interests could interfere with the judgment of *personnel* (3.24) in carrying out their duties for the organization

3.30
due diligence
process (3.14) to further assess the nature and extent of the bribery *risk* (3.11) and help organizations make decisions in relation to specific transactions, projects, activities, business associates and personnel

3.31
ensure
take reasonable and proportionate steps with the intent of achieving the stated objective

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal factors that are relevant to its purpose and that affect its ability to achieve the objectives of its anti-bribery management system. These factors will include, without limitation, the following:

a) size and structure of the organization;

b) locations and sectors in which the organization operates or anticipates operating;

c) nature, scale and complexity of the organization's activities and operations;

d) entities over which the organization has control;

e) organization's business associates;

g) applicable statutory, regulatory, contractual and professional obligations and duties.

NOTE An organization has control over another organization if it directly or indirectly controls the management of the organization.

4.2 Understanding the needs and expectations of stakeholders

The organization shall determine:

a) the stakeholders that are relevant to the anti-bribery management system;

b) the relevant requirements of these stakeholders.

NOTE In identifying the requirements of stakeholders, an organization can distinguish between mandatory requirements and the non-mandatory expectations of, and voluntary commitments to, stakeholders.

4.3 Determining the scope of the anti-bribery management system

The organization shall determine the boundaries and applicability of the anti-bribery management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal factors 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.

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 International Standard.

The anti-bribery management system shall contain measures designed to identify and evaluate the risk of, and to prevent, detect and address, 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 A.3 for guidance.

4.5 Bribery risk assessment

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

a) identify the bribery risks the organization might reasonably anticipate given the factors listed in 4.1;

b) 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

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 maintain documented information that demonstrates that the bribery risk assessment has been conducted, and used to design the anti-bribery management system.

NOTE See A.4 for guidance.

5 Leadership

5.1 Leadership and commitment

5.1.1 Governing body

When the organization has a governing body, that body shall demonstrate leadership and commitment with respect to the anti-bribery management system by:

a) approving the organization's anti-bribery policy;

b) at planned intervals receiving and reviewing information about the content and operation of the organization's anti-bribery management system;

c) ensuring that adequate and appropriate resources needed for effective operation of the anti-bribery management system are allocated and assigned;

d) exercising reasonable oversight over the implementation of the organization's anti-bribery management system by top management and its effectiveness.

NOTE These activities shall be carried out by top management if the organization does not have a governing body.

5.1.2 Top management

Top management shall demonstrate leadership and commitment with respect to the anti-bribery management system by:

a) ensuring that the anti-bribery management system, including policy and objectives, is established, implemented, maintained and reviewed to adequately address the organization's bribery risks;

b) ensuring the integration of the anti-bribery management system requirements into the organization's processes;

c) deploying adequate and appropriate resources for the effective operation of the anti-bribery management system;

d) communicating internally and externally regarding the anti-bribery policy;

e) communicating internally the importance of effective anti-bribery management and of conforming to the anti-bribery management system requirements;

f) ensuring that the anti-bribery management system is appropriately designed to achieve its objectives;

g) directing and supporting personnel to contribute to the effectiveness of the anti-bribery management system;

h) promoting an appropriate anti-bribery culture within the organization;

j) supporting other relevant management roles to demonstrate their leadership in preventing and detecting bribery as it applies to their areas of responsibility;

k) encouraging the use of reporting procedures for suspected and actual bribery (see also 8.9);

l) ensuring that no personnel will suffer retaliation or discriminatory or disciplinary action for reports made in good faith or on the basis of a reasonable belief of violations or suspected violations of the organization's anti-bribery policy, or for refusing to engage in bribery, even if such refusal may result in the organization losing business (except where the individual participated in the breach);

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

NOTE See A.5 for guidance.

5.2 Anti-bribery policy

Top management shall establish, review and maintain 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 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; and

i) explains the consequences of not complying with the anti-bribery policy.

The anti-bribery policy shall:

a) be available as documented information;

b) be communicated in appropriate languages within the organization and to business associates who pose more than a low risk of bribery;

c) 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 ensuring that the anti-bribery management system

requirements are applied and complied with in their department or function.

the organization.

5.3.2 Anti-bribery compliance function

Top management shall assign to an anti-bribery compliance function the responsibility and authority for:

a) overseeing the design and implementation by the organization of the anti-bribery management system;

b) providing advice and guidance to personnel on the anti-bribery management system and issues relating to bribery;

c) ensuring that the anti-bribery management system conforms to the requirements of this International Standard;

d) reporting on the performance of the anti-bribery management system to the governing body (if any) and top management and other compliance functions, as appropriate.

The anti-bribery compliance function shall be adequately resourced and assigned to person(s) who have the appropriate competence, status, and independence.

The anti-bribery compliance function shall have direct and prompt access to the governing body (if any) and top management in the event that any issue or concern needs to be raised in relation to bribery or the anti-bribery management system.

Top management may assign some or all of the anti-bribery compliance function to persons external to the organization. If it does, top management shall ensure that specific personnel have responsibility for and authority over those assigned parts of the function.

NOTE See A.6 for guidance.

5.3.3 Delegated decision-making

Where top management delegates to personnel the responsibility or authority for the making of decisions in relation to which there is more than a low risk of bribery, the organization shall establish and maintain a decision-making process or set of controls that requires that the decision process and the level of authority of the decision-maker(s) are appropriate and free of actual or potential conflicts of interest. Top management shall ensure that these processes are reviewed periodically as part of its roles and responsibilities for implementation of and compliance with the anti-bribery management system outlined in section 5.3.1.

NOTE 1 In delegating responsibility and authority, top management should identify and take steps to manage actual or potential conflicts of interest.

NOTE 2 Delegation of decision-making will not exempt top management or the governing body of their duties and responsibilities as described in sections 5.1.1, 5.1.2 and 5.3.1. Nor will it necessarily transfer to the delegated personnel potential legal responsibilities.

6 Planning

6.1 Actions to address bribery risks and opportunities

When planning for the anti-bribery management system, the organization shall consider the factors referred to in 4.1, the requirements referred to in 4.2, the risks identified in 4.5, and opportunities that need to be addressed to:

a) give reasonable assurance that the anti-bribery management system can achieve its objectives;

b) prevent, or reduce, undesired effects relevant to the anti-bribery policy and objectives;

c) monitor the effectiveness of the anti-bribery management system;

The organization shall plan:

a) actions to address these bribery risks and opportunities;

b) how to:

1) integrate and implement these actions into its anti-bribery management system processes;

2) evaluate the effectiveness of these actions.

6.2 Anti-bribery objectives and planning to achieve them

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

The anti-bribery 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;

g) be updated as appropriate.

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

When planning how to achieve its anti-bribery 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.

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 A.7 for guidance.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its anti-bribery performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire and maintain the necessary competence, and evaluate the effectiveness of the actions taken;

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example, the provision of training to, the coaching of, or the re-assignment of personnel or business associates; or the hiring or contracting of competent persons or business associates.

7.2.2 Employment procedures

7.2.2.1 In relation to all of its personnel, the organization shall implement procedures such that:

a) conditions of employment require personnel to comply with the anti-bribery policy and anti-bribery management system, and give the organization the right to discipline personnel in the event of non-compliance;

b) within a reasonable period of their employment commencing, personnel receive a copy of, or are provided with access to, the anti-bribery policy and training in relation to that policy;

c) the organization has procedures which enable it to take appropriate disciplinary action against personnel who breach the anti-bribery policy and anti-bribery management system; and

d) personnel are not penalized (e.g. by demotion, preventing advancement, disciplinary action, transfer, dismissal, bullying or victimization):

   1) for refusing to participate in, or for turning down, any activity in respect of which they have reasonably judged there to be a more than low risk of bribery which has not been mitigated by the organization; or

   2) for concerns raised or reports made in good faith or on the basis of a reasonable belief, of attempted, actual or suspected bribery or breaches of the anti-bribery policy or the anti-bribery management system (except where the individual participated in the breach).

7.2.2.2 In relation to all personnel in positions which are exposed to more than a low bribery risk as determined in the bribery risk assessment (4.5), and to all personnel employed in the anti-bribery compliance function the organization shall implement procedures which provide that:

a) due diligence (see 8.2) is conducted on persons before they are employed, and on personnel before they are transferred or promoted by the organization, to ascertain as far as is reasonable that it is appropriate to employ or redeploy them and that it is reasonable to believe that they will comply with the anti-bribery policy and anti-bribery management system requirements;

b) performance bonuses, performance targets and other incentivizing elements of remuneration are reviewed periodically to verify that there are reasonable safeguards in place to prevent them from encouraging bribery;

c) such personnel, top management, ~~as well as~~ 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

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 and 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 they can help prevent and avoid bribery and recognize key bribery risk indicators;

e) their contribution to the effectiveness of the anti-bribery management system, including the benefits of improved anti-bribery performance and of reporting suspected bribery;

f) the implications and potential consequences of not conforming with the anti-bribery management system requirements;

g) how and to whom they should report any concerns (see 8.9);

h) 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 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 retained for that purpose.

NOTE 2 See 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:

a) on what it will communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate;

f) the languages in which to communicate.

7.4.2 The anti-bribery policy shall be made available to all the organization's personnel and business associates, be communicated directly to both personnel and business associates who pose more than a low risk of bribery, and shall be published through the organization's internal and external communication channels as appropriate.

7.5 Documented information

7.5.1 General

The organization's anti-bribery management system shall include:

a) documented information required by this International Standard;

b) documented information determined by the organization as being necessary for the effectiveness of the anti-bribery management system.

NOTE 1 The extent of documented information for an anti-bribery management system can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of personnel.

NOTE 2 Documented information can be retained separately as part of the anti-bribery management system, or can be maintained as part of other management systems (e.g. compliance, financial, commercial, audit etc.), and subject to the document retention policy of the organization.

NOTE 3 See A.17 for guidance.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic);

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the anti-bribery management system and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

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);

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, monitor 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.

8.2 Due diligence

Where the organization's bribery risk assessment 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 may conclude that it is unnecessary, unreasonable or disproportionate to undertake due diligence on certain categories of personnel and business associate.

NOTE 2 The factors listed in a), b) and c) above are not exhaustive.

NOTE 3 See A.10 for guidance.

8.3 Financial controls

The organization shall implement financial controls that manage bribery risk.

NOTE See A.11 for guidance.

8.4 Non-financial controls

NOTE 1 Any one transaction, activity or relationship can be subject to financial as well as non-financial controls.

NOTE 2 See A.12 for guidance.

8.5 Implementation of anti-bribery controls by controlled organizations and by business associates

8.5.1 The organization shall implement procedures which require that all other organizations over which it has control either:

a) implement the organization's anti-bribery management system; or

b) implement their own anti-bribery controls,

in each case only to the extent that is reasonable and proportionate having regard to the bribery risks which the controlled organizations face, taking into account the bribery risk assessment conducted pursuant to 4.5.

NOTE An organization has control over another organization if it directly or indirectly controls the management of the organization.

8.5.2 In relation to business associates not controlled by the organization for which the bribery risk assessment (see 4.5) or due diligence (see 8.2) has identified a more than low bribery risk, and where anti-bribery controls implemented by the business associates would help mitigate the relevant bribery risk, the organization shall implement procedures as follows:

a) the organization shall determine whether the business associate has in place anti-bribery controls which manage the relevant bribery risk.

b) where a business associate does not have in place anti-bribery controls, or it is not possible to verify whether it has them in place:

1) the organization shall where practicable require the business associate to implement anti-bribery controls in relation to the relevant transaction, project or activity, or

2) where it is not practicable to require the business associate to implement anti-bribery controls, the organization shall take this factor into account when assessing the bribery risks that the business associates pose, and the way in which the organization manages such risks.

NOTE See A.13 for guidance

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 is practicable:

a) business associates commit to prevent bribery by or 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 or 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, then 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).

NOTE See A.14 for guidance

763 **8.7 Gifts, hospitality, donations and similar benefits**

766 or could reasonably be perceived as bribery.

767 NOTE See A.15 for guidance

768 **8.8 Managing inadequacy of anti-bribery controls**

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

773 a) in the case of an existing transaction, project, activity or relationship, take steps appropriate to the bribery
774 risks and the nature of the transaction, project, activity or relationship to terminate, discontinue, suspend
775 or withdraw from it as soon as is practicable;

776 b) in the case of a proposed new transaction, project, activity or relationship, postpone or decline to continue
777 with it.

778 **8.9 Raising concerns**

779 The organization shall implement procedures which:

780 a) enable persons to report attempted, suspected and actual bribery, or any breach of or weakness in the
781 anti-bribery management system, to the anti-bribery compliance function or to appropriate personnel
782 (either directly or through an appropriate third party);

783 b) except to the extent required to progress an investigation or by law, require that the organization treats
784 reports confidentially so as to protect the identity of the reporter and of others involved or referenced in
785 the report

786 c) allow anonymous reporting;

787 d) prohibit retaliation, and protect personnel from retaliation, after such personnel have in good faith or on
788 the basis of a reasonable belief raised or reported a concern about attempted, actual or suspected
789 bribery or breaches of the anti-bribery policy or the anti-bribery management system;

790 e) enable personnel to receive advice from an appropriate person on what to do if faced with a concern or
791 situation which could involve bribery;

792 f) encourage the use by personnel of the reporting procedures.

793 The organization shall ensure that all personnel are aware of the reporting procedures, and are able to use
794 them, and are aware of their rights and protections under the procedures.

795 NOTE 1 These procedures can be the same as, or form part of, those used for the reporting of other issues of concern
796 (e.g. safety, malpractice, wrongdoing or other serious risk).

797 NOTE 2 The organization can use another organization to manage the reporting system on its behalf.

798 **8.10 Investigating and dealing with bribery**

799 The organization shall implement procedures which:

800 a) require assessment and, where appropriate, investigation of bribery, or breach of the anti-bribery policy or
801 the anti-bribery management system , which is reported, detected or reasonably suspected;

802 b) require appropriate action in the event that the investigation reveals bribery, or breach of the anti-bribery
803 policy or the anti-bribery management system;

c) empower and enable investigators and require co-operation in the investigation by relevant personnel;

and other compliance functions, as appropriate.

The investigation should be carried out by and reported to personnel who are not part of the role or function being investigated. The organization may appoint another organization to conduct the investigation and report the results to personnel who are not part of the role or function being investigated.

NOTE 1 See A.18 for guidance

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) when the monitoring and measuring shall be performed;

d) when the results from monitoring and measurement shall be analysed and evaluated;

e) to whom such information shall be provided.

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 of the anti-bribery management system.

NOTE See A.19 for guidance.

9.2 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; and

b) being effectively implemented.

The anti-bribery compliance function shall report at planned intervals and on an ad-hoc basis, if required, 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 the report will depend on the organization's requirements, but is recommended to be at least annually.

NOTE 2 The organization can use another organization to assist in the review, as long as the other organization's observations are appropriately communicated to the anti-bribery compliance function.

9.3 Internal audit

9.3.1 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;

b) is effectively implemented and maintained.

NOTE 1 Guidance on auditing management systems can be obtained from 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.

9.3.2 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, top management and the anti-bribery compliance function;

e) retain documented information as evidence of the implementation of the audit programme and the audit results.

9.3.3 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) non-compliance with the anti-bribery policy or anti-bribery management system requirements;

c) failure of business associates to conform to the applicable requirements of the organization; and

d) weaknesses in or opportunities for improvement to the anti-bribery management system.

9.3.4 To ensure the objectivity and impartiality of these audit programmes, the organization shall ensure that these audits are undertaken by:

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

b) the anti-bribery compliance function (unless the scope of the audit includes an evaluation of the anti-bribery management system itself, or similar work for which the anti-bribery compliance function is responsible); or

c) an appropriate person from a department or function other than the one being audited; or

d) an appropriate third party; or

e) a group comprising any of a) to d).

The organization shall ensure that no auditor is auditing his or her own area of work.

NOTE See A.16 for guidance.

9.4 Top management review

Top management shall review the organization's anti-bribery management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The top management review shall include consideration of:

b) changes in external and internal factors that are relevant to the anti-bribery management system;

c) information on the performance of the anti-bribery system, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) reports of bribery;

5) investigations;

6) the nature and extent of the bribery risks faced by the organization;

i) effectiveness of actions taken to address bribery risks;

j) opportunities for continual improvement of the anti-bribery management system, as referred to in 10.2.

The outputs of the top management review shall include decisions related to continual improvement opportunities and any need for changes to the anti-bribery management system.

A summary of the results of the top management review shall be reported to the governing body.

The organization shall retain documented information as evidence of the results of top management reviews.

9.5 Governing body review

The governing body (if any) shall undertake periodic reviews of the anti-bribery management system based upon information provided by top management and the anti-bribery compliance function and any other information that the governing body may request or obtain.

The organization shall retain summary documented information as evidence of the results of governing body reviews.

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 causes 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;

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.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the anti-bribery management system.

Annex A

Guidance on the use of this International Standard

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 may 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 International Standard. The actual steps which the organization takes should be reasonable and proportionate having regard to the nature and extent of bribery risks which the organization faces (see 4.5, and the factors in 4.1 and 4.2).

Some internationally recognised publications which comment on best practice are referred to in the Bibliography.

A.2 Scope of the anti-bribery management system

A.2.1 Standalone or integrated anti-bribery management system

The organization may 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 may also choose to implement this anti-bribery management system alongside or as part of its other management systems, such as quality, environmental and safety (in which case the organization can refer to ISO 9001, ISO 14001, 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 which 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 International Standard, and therefore 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 standard. 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. Therefore, 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 may be faced with requests or demands for such payments on how to avoid them and deal with them. Such guidance could include, for example:

a) specifying action to be taken by any personnel faced with a demand for payment, such as:

   1) in the case of a facilitation payment, asking for proof that the payment is legitimate, and an official receipt for payment and, if no satisfactory proof is available, refusing to make the payment;

   2) in the case of an extortion payment, making the payment if their health, safety or liberty, or that of another, is threatened;

b) specifying action to be taken by personnel who have made a facilitation or extortion payment:

1) making a record of the event;

k) specifying action to be taken by the organization when personnel have made a facilitation or extortion payment:

1) appointing an appropriate manager to investigate the event (preferably the anti-bribery compliance function or a manager who is independent from the personnel's department or function);

2) correctly recording the payment in the organization's accounts;

3) if appropriate, or if required by law, reporting the payment to the relevant authorities.

A.3 Reasonable and proportionate

A.3.1 Bribery is normally concealed. It can be difficult to prevent, detect and address. Recognising these difficulties, the overall intent of this International Standard is that the governing body (if any) and top management of an organization need to have a genuine commitment to prevent, detect and address bribery in relation to the organization's business or activities and need to, with genuine intent, implement measures in the organization which are designed to prevent, detect and address bribery. The measures cannot be so expensive, burdensome and bureaucratic that they are unaffordable or bring the business to a halt. Nor can they be so simple and ineffective that bribery can easily take place. The measures need to be appropriate to the bribery risk, and should have a reasonable chance of being successful in their aim of preventing, detecting and addressing bribery.

A.3.2 While the types of anti-bribery measures that need to be implemented are reasonably well recognised by international good practice, and some of which are reflected as requirements in this International Standard, the actual detail of the measures to be implemented differ widely according to the relevant circumstances. Therefore, it is impossible to prescribe exactly in any detail what an organization should do in any particular circumstance. The reasonable and proportionate qualification has been introduced into this International Standard, so that every circumstance can be judged on its own merit.

A.3.3 The following examples provide some guidance on how the reasonable and proportionate qualification may apply in relation to differing circumstances:

a) A very large multi-national organization may need to deal with multiple layers of management, and thousands of personnel. Its anti-bribery management system will therefore typically need to be far more detailed than that of a small organization with only a few personnel.

b) An organization which has activities in a higher bribery risk location will normally need more comprehensive bribery risk assessment and due diligence procedures and a higher level of anti-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 all 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 may conclude, as part of its bribery risk assessment, that certain categories of business associates, such as retail customers, may not 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 all 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 may accept the fact of bribery occurring. That is, the risk of bribery

occurring (i.e., whether a bribe might occur) is not the same as the occurrence of a bribe (the fact of the

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 system will focus on; that is, the bribery risks deemed by the organization to be a priority for bribery risk mitigation, control implementation, and allocation of 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"), though in so doing the organization should take into account its anti-bribery policy and objectives. The following provides an example of how an organization may choose to undertake this assessment:

a) Select bribery risk evaluation criteria. For example, the organization may select a 3 tier criteria such as "low", "medium", "high", a more detailed 5 or 7 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 may pose. An appropriate bribery index can be used to assist in this assessment. Locations or sectors with a higher risk of bribery may be deemed by the organization e.g. as "medium" or "high" risk, which may result in the organization imposing a higher level of controls applicable to activities by the organization in those locations or sectors.

d) Examine the nature, scale and complexity of the organization's types of activities and operations.

    1) It may for example be easier to control bribery risk where an organization undertakes a small manufacturing operation in one location than where an organization is involved in numerous large construction projects in several locations.

    2) Some activities may carry specific bribery risks. For example, offset arrangements by which the government of a country purchasing products or services requires the supplier to reinvest some proportion of the value of the contract in the purchasing country. The organization should take appropriate steps to ensure that the offset arrangements do not constitute bribery.

e) Examine the organization's existing and potential types of business associates by category, and assess the bribery risk in principle which they pose. For example:

    1) The organization may have large numbers of customers who purchase very low value products from the organization, and who in practice pose a minimal bribery risk to the organization. In this case the organization may deem these customers low bribery risk, and may determine that these customers will not need to have any specific anti-bribery controls related to them. Alternatively, the organization may deal with customers who buy very large value products from the organization, and may pose a significant bribery risk (e.g. the risk of demanding bribes from the organization in return for payments, approvals etc). These types of customers may be deemed e.g. as "medium" or "high" bribery risk, and therefore require a higher level of anti-bribery controls by the organization.

    2) Different categories of suppliers can pose different levels of bribery risk. For example, suppliers with a very large scope of work, or who may be in contact with the organization's clients, customers or relevant public officials, may pose a "medium" or "high" bribery risk. Some categories of suppliers may be "low" risk, e.g. suppliers based in low bribery risk locations which have no interface with

public officials relevant to the transaction or the organization's clients or customers. Some categories

suppliers.

3) Agents or intermediaries who interact with the organization's clients or public officials on behalf of the organization are likely to pose a "medium" or "high" bribery risk, particularly if they are paid on a commission or success fee basis.

l) Examine the nature and frequency of interactions with domestic or foreign public officials who can pose a bribery risk. For example, interactions with public officials responsible for issuing permits and approvals can pose a bribery risk.

m) Examine applicable statutory, regulatory, contractual and professional obligations and duties, such as for example the prohibition or limitation of entertainment of public officials or of the use of agents.

h) Consider the extent to which the organization is able to influence or control the assessed risks.

The above bribery risk factors inter-relate. For example, suppliers in the same category may pose a differing bribery risk depending on the location in which they operate.

A.4.2 Having assessed the relevant bribery risks, the organization can then determine the type and level of anti-bribery controls being applied to each risk category, and can assess whether existing controls are adequate. If not, the controls can be appropriately improved. For example, a higher level of control is likely to be implemented with respect to higher bribery risk locations and higher bribery risk categories of business associate. The organization may determine that it is acceptable to have a low level of control over low bribery risk activities or business associates. Some of the requirements in this standard expressly exclude the need to apply those requirements to low bribery risk activities or business associates (although the organization may choose to apply them if it wishes).

A.4.3 The organization may 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 risk controls.

A.4.4 This bribery risk assessment exercise is not meant to be an extensive or overly complex exercise. Nor are the results of the assessment necessarily going to be proven to be correct (e.g. a transaction assessed as low bribery risk may 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, circumstances (e.g. new markets or products, legal requirements, experiences gained, etc.).

NOTE Further guidance can be found 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, such as 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, etc.) who are referred to in this International Standard as "top management". Therefore, with respect to the anti-bribery management system, the governing body should be knowledgeable about the content and operation of the system, and should exercise reasonable oversight with respect to the adequacy, effectiveness and implementation of the system. It should regularly receive information regarding the performance of the system through the management review process (this might be to the entire governing body, or to a committee of the authority, such as the audit committee). In that regard, the anti-bribery compliance function should be able to report information about the system directly to the governing body (or the appropriate committee thereof).

A.5.2 Some organizations, particularly smaller ones, may not have a separate governing body or the roles of the governing body and executive management may be combined in one group or even one individual. In

this case, the group or individual will have the responsibilities allocated in this International Standard to 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 can combine this responsibility with other responsibilities. Where the extent of bribery risk and resultant work load justifies it, the anti-bribery compliance function may 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 may assign responsibility to a committee that embodies a range of relevant expertise. Some organizations may 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 The standard requires that the anti-bribery compliance function shall be staffed by person(s) who have the appropriate competence, status, authority and independence. In this respect:

a) "Competence" means that the relevant person(s) assigned the anti-bribery compliance responsibility has the personal ability to deal with the requirements of the role, and the capacity to learn about the role and perform it appropriately.

b) "Status" means that other personnel are likely to listen to and respect the opinions of the person assigned compliance responsibility.

c) "Authority" means that the relevant person(s) assigned the compliance responsibility is granted sufficient powers by the governing body (if any) and top management so as to be able to undertake the compliance responsibilities effectively.

d) "Independence" means that the relevant person(s) assigned the compliance responsibility is as far as possible not personally involved in the activities of the organization which are exposed to bribery risk. This can more easily be achieved where the organization has appointed a person to handle the role full time, but is more difficult for a smaller organization which has appointed a person to combine the compliance role with other functions. Where the anti-bribery compliance function is part time, the role should not be performed by an individual who may be exposed to bribery while performing their primary function. In the case of a very small organization where it may be more difficult to achieve independence, the appropriate person should, to the best of their ability, separate their other responsibilities from their compliance responsibilities so as to be impartial.

A.6.3 It is important that the anti-bribery compliance function has direct access to top management and, if the organization has one, to the governing body, in order to communicate relevant information. The function should not have to report solely to another manager in the chain who then reports to top management, as this increases the risk that the message given by the anti-bribery compliance function is not fully or clearly received by top management. The anti-bribery compliance function should also have a direct communications relationship to the governing body (if one exists), without having to go through top management. This can either be to the fully constituted governing body (e.g. a board of directors or a supervisory council) or can be to a specially delegated committee of the governing body or top management (e.g. an audit or ethics committee).

A.6.4 The primary responsibility of the anti-bribery compliance function is overseeing the design and implementation of the anti-bribery management system. This should not be confused with direct responsibility for the anti-bribery performance of the organization and compliance with applicable anti-bribery laws. Everyone is responsible for conducting themselves in an ethical and compliant manner, including conforming to the requirements of the organization's anti-bribery management system and anti-bribery laws. It is particularly important that management take the leadership role in achieving compliance in the parts of the organization for which they have responsibility.

NOTE Further guidance can be found in ISO 19600.

A.7 Resources

a) **Human resources:** ensuring that sufficient personnel are able to apply sufficient time to their relevant anti-bribery responsibilities so that the anti-bribery management system can function effectively. This includes assigning sufficient person(s) (either internal or external) to the anti-bribery compliance function.

b) **Physical resources:** ensuring that the necessary physical resources are made available in the organization, including to the anti-bribery compliance function, so that the anti-bribery management system can function effectively. For example, office space, furniture, computer hardware and software, training materials, telephones, stationery etc.

c) **Financial resources:** ensuring that a sufficient budget is made available, including to the anti-bribery compliance function, so that the anti-bribery management system can function effectively.

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, may 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) ensuring 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 proportionate 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). Therefore, 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 breaching 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 may result in disciplinary action.

A.8.3 Conflicts 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.

A.8.4 Bribery of the organization's personnel

A.8.4.1 The measures necessary to prevent, detect and address the risk of the organization's personnel bribing others on behalf of the organization ("outbound bribery") may be different from the measures used to prevent, detect and address the risk of bribery of the organization's personnel ("inbound bribery"). For example, the ability to identify and mitigate inbound bribery risk may be significantly restricted by the availability of information that is not under the control of the organization (e.g. employee personal bank account and credit card transaction data), applicable law (e.g. privacy law), or other factors. As a result, the number and types of controls available to the organization to mitigate the risk of outbound bribery will outweigh the number of controls it can implement to mitigate the risk of inbound bribery.

A.8.4.2 Bribery of the organization's personnel is most likely to occur in relation to personnel who are able to make or influence decisions on behalf of the organization (e.g. a procurement manager who can award contracts, a supervisor who can approve work done, a manager who can appoint personnel or approve salaries or bonuses, a clerk who prepares documents for granting of licenses, permits etc.). As the bribe is likely to be accepted by personnel outside of the scope of the organization's systems of controls, the ability of the organization to prevent or detect these bribes can be limited.

A.8.4.3 In addition to the steps referred to in A.8.1 and A.8.3, the risk of inbound bribery could be mitigated by the following requirements of this standard dealing with this risk:

a) the organization's anti-bribery policy (5.2) should clearly prohibit solicitation and acceptance of bribes by the organization's personnel and anyone working on behalf of the organization.

b) guidance and training materials (7.3) should reinforce the prohibition on soliciting and accepting bribes, and include:

    1) guidance for reporting bribery concerns (8.9);

    2) emphasis on the organization's non-retaliation policy (8.9).

c) the organization's gifts and hospitality policy (8.7) should limit the acceptance by personnel of gifts and hospitality.

d) the publication of the organization's anti-bribery policy and reporting information on the organization's website helps to set expectations with business associates, so as to decrease the likelihood that business associates will offer, or the organization's personnel will solicit or accept, a bribe.

e) controls (8.4) requiring e.g. the use of approved suppliers, competitive bidding, at least two signatures on contract awards, work approvals etc. reduce the risk of corrupt awards or approvals.

A.8.4.4 The organization may also implement audit procedures to identify ways personnel may exploit existing control weaknesses for personal gain. Example procedures could include:

a) reviewing payroll files for phantom and duplicate personnel records;

b) reviewing personnel expense reports to identify unusual spending;

c) comparing personnel payroll file information (e.g. personal bank account numbers and addresses) with

A.8.5 Temporary staff or workers

In some cases, temporary staff or workers may be provided to the organization by a labour supplier or other organization. In this case, the organization should determine whether the bribery risk posed 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 organization which provides the temporary staff or workers.

A.9 Awareness and training

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

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, investigative 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 on-line module, or by face to face methods (e.g. classroom sessions, workshops, roundtable discussions between relevant personnel, or by one-to-one sessions). Therefore, 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 and top management, 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 compliance function adequately.

A.9.5 The training could 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 breach. 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 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. Therefore, 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. Thus, this portion of the standard 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. The organization can communicate these obligations to its

account, among other things, the results of the bribery risk assessment. The level of detail of the procedures and the output of these procedures (including records) will depend upon the specific circumstances of the organization and its business associates.

A.10 Due diligence

A.10.1 The purpose of conducting due diligence on certain transactions, projects, activities, business associates, or an organization's personnel is to further evaluate the scope, scale, and nature of the more than low bribery risks identified as part of the organization's risk assessment (4.5). It also serves the purpose of acting as an additional, targeted control in the prevention and detection of bribery risk, and informs the organization's decision on whether to postpone, discontinue, or revise those transactions, projects, or relationships with business associates or personnel.

A.10.2 Factors which the organization may find useful to evaluate in relation to a business associate include:

a) whether the business associate is a legitimate business entity, as demonstrated by indicators such as corporate registration documents, annual filed accounts, tax identification number, listing on a stock exchange;

b) whether the business associate has the qualifications, experience and resources needed to conduct the business for which it is being contracted;

c) whether and to what extent the business associate has an anti-bribery management system;

d) whether the business associate has a reputation for bribery, fraud, dishonesty or similar misconduct, or has been investigated, convicted, sanctioned or debarred for bribery or similar criminal conduct;

e) the identity of the shareholders (including the ultimate beneficial owner(s)) and top management of the business associate, and whether they:

   1) have a reputation for bribery, fraud, dishonesty or similar misconduct;

   2) have been investigated, convicted, sanctioned or debarred for bribery or similar criminal conduct;

   3) 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.);

f) structure of the transaction and payment arrangements.

A.10.3 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.

A.10.4 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.

A.10.6 Different types of business associates are likely to require different levels of due diligence. For example:

a) 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

b) the level of influence which the organization has over its business associates also affects the extent of due diligence which the organization can reasonably undertake. 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).

A.10.7 The due diligence undertaken by the organization on its business associates may include, for example:

a) a questionnaire sent to the business associate in which it is asked to answer the questions referred to in A.10.2;

b) a web-search on the business associate and its shareholders and top management to identify any bribery-related information;

c) searching appropriate government, judicial, and international resources for relevant information;

d) checking publically available debarment lists of organizations who 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;

e) making enquiries of appropriate other parties about the business associate's ethical reputation;

f) appointing other persons or organizations with relevant expertise to assist in the due diligence process.

A.10.8 The business associate can be asked further questions based on the results of the initial due diligence (for example, to explain any adverse information).

A.10.9 Due diligence is not a perfect tool. The absence of negative information does not necessarily mean that the business associate does not pose a bribery risk. Negative information does not necessarily mean that the business associate poses a bribery risk. However, the results need to be carefully assessed and a rational judgement made by the organization based on the facts available to it. The overall intent is that the organization makes reasonable and proportionate enquiries about the business associate, taking into account the activities that the business associate would undertake and the bribery risk inherent in these activities, so as to form a reasonable judgment on the level of bribery risk which the organization is exposed to if it works with the business associate.

A.10.10 Due diligence on personnel is covered in A.8.1.

A.11 Financial controls

Financial controls are the management systems and processes implemented by the organization to manage its financial transactions properly and to record these transactions accurately, completely and in a timely manner. Depending on the size of the organization and transaction, the financial controls implemented by an organization which can reduce the bribery risk could include, for example:

a) implementing a separation of duties, so that the same person cannot both initiate and approve a payment;

b) implementing appropriate tiered levels of authority for payment approval (so that larger transactions require more senior management approval);

c) ensuring that the payee's appointment and work or services carried out have been approved by the

e) requiring the appropriate supporting documentation to be annexed to payment approvals;

f) restricting the use of cash and implementing effective cash control methods;

g) ensuring that payment categorizations and descriptions in the accounts are accurate and clear;

h) implementing periodic management review of significant financial transactions;

i) implementing periodic and independent financial audits and changing, on a regular basis, the person or the organization who carries out the audit.

A.12 Non-financial controls

Non-financial controls are the management systems and processes implemented by the organization to help it ensure that its procurement, operational, commercial and other non-financial aspects are being properly managed. Depending on the size of the organization and transaction, the procurement, operational, commercial and other non-financial controls implemented by an organization which can reduce bribery risk could include, for example:

a) using approved sub-contractors, suppliers and consultants that have undergone a pre-qualification process under which the likelihood of their participating in bribery is assessed; this process is likely to include due diligence of the type specified in A.10;

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; and

3) whether any payments to be made to the business associate are reasonable and proportionate 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 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.

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

approval ladders, checklists, forms, IT-workflows).

Further examples of controls and guidance can be found in ISO 19600.

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

A.13.1 General

A.13.1.1 The reason for this requirement (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;

d) a client of the organization requiring the organization to appoint a specific sub-contractor or supplier in circumstances where a manager of the client or public official may benefit personally from the appointment;

e) an agent of the organization paying a bribe to a manager of the organization's customer on behalf of the organization;

f) a supplier or sub-contractor to the organization paying a bribe to the organization's procurement manager in return for a contract award.

A.13.1.2 If the controlled organization or business associate has implemented anti-bribery controls in relation to those risks, then the consequent bribery risk to the organization is normally reduced.

A.13.1.3 This requirement in 8.5 distinguishes between those organizations over which the organization has control, and those over which it does not. For the purposes of this requirement, an organization has control over another organization if it directly or indirectly controls the management of the organization. An organization might have control, for example, over a subsidiary, joint venture or consortium through majority votes on the board, or through a majority shareholding. The organization does not have control over another organization for the purposes of this requirement merely because it places a large amount of work with that other organization.

A.13.2 Controlled organizations

A.13.2.1 It is reasonable to expect the organization to ensure that any other organization which it controls implements reasonable and proportionate anti-bribery controls. This could either be by the controlled organization implementing the same anti-bribery management system as implemented by the organization, or by the controlled organization implementing its own specific anti-bribery controls. These controls should be reasonable and proportionate having regard to the bribery risks which the controlled organization faces, taking into account the bribery risk assessment conducted pursuant to 4.5.

A.13.2.2 Where a business associate is controlled by the organization (e.g. a joint venture over which the organization has management control) then that controlled business associate would fall under the requirements in 8.5.1

A.13.3 Business associates

bribery, or that anti-bribery controls implemented by the business associates would not help mitigate the relevant bribery risk, then the organization does not need to take the steps required by 8.5.2 to require implementation by the business associate of anti-bribery controls. This reflects the reasonableness and proportionality of the standard. It should be noted that there are two scenarios in this category:

a) where the business associate poses no or a low risk of bribery; or

b) where the business associate poses more than a low bribery risk, but controls that could be implemented by the business associate would not help mitigate the relevant risk. There would be no point in insisting that the business associate implements controls which would not help. However, in this case, the organization would be expected to take account of this factor in its risk assessment in order to inform the decision regarding how and whether to proceed with the relationship.

A.13.3.2 If the bribery risk assessment (4.5) or due diligence (8.2) concludes that the non-controlled business associate poses more than a low risk of bribery, and that anti-bribery controls implemented by the business associate would help mitigate this bribery risk, then the organization takes the following further steps under 8.5:

a) The organization shall determine 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. This due diligence could include, for example, requiring the business associate to declare to the organization (in a meeting or in writing) whether or not it has appropriate controls in place, describe what these controls are, and provide appropriate copy documentation to verify that it does have these controls. 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 steps that the organization needs to take to verify these controls, and the extent of the 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, then the requirement of 8.5 is addressed in relation to that business associate. See A.13.8 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 which manage the relevant bribery risks, or if it is not possible to verify whether it has these controls in place, then the organization undertakes the following further steps:

    1) If it is practicable (see A.13.7) to do so, the organization shall require the business associate to implement anti-bribery controls (see A.13.8) in relation to the relevant transaction, project or activity.

    2) Where it is not practicable (see A.13.7) to require the business associate to implement anti-bribery controls, the organization shall take this factor into account when assessing the bribery risks that the business associates pose, 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) then 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

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 (for example, 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) In the case of a major high bribery risk business associate with a large and complex scope of work, the organization might require the business associate to have implemented controls equivalent to those required by this International Standard relevant to the bribery risks it poses to the organization.

b) In the case of a medium size and medium bribery risk business associate, the organization may require the business associate to have implemented some minimum anti-bribery requirements in relation to the transaction, such as an anti-bribery policy, training for its relevant employees, a manager with responsibility for compliance in relation to the transaction, controls over key payments and a reporting line.

c) In the case of small business associates who have a very specific scope of work (for example an agent or a minor supplier), the organization may require training for relevant employees, and controls over key payments and gifts and hospitality.

The controls only need to operate in relation to the transaction between the organization and business associate (although in practice the business associate may have controls in place in relation to its whole business).

The above are examples only. The important issue is for the organization to identify the key bribery risks in relation to the transaction, and to require as far as practicable that the business associate has implemented reasonable and proportionate controls over those key bribery risks.

A.13.3.5 The organization will normally impose these requirements over the non-controlled business associate as a pre-condition to working with the business associate and/or as part of the contract document.

A.13.3.6 The organization is not required to verify full compliance by the non-controlled business associate with these requirements. However, the organization should take reasonable steps to satisfy itself that the business associate is complying (e.g. by requesting the business associate to provide copies of its relevant policy documents). In high bribery risk cases (e.g. an agent), the organization may implement monitoring procedures including e.g. reporting and audit rights.

A.13.3.7 As anti-bribery controls can take some time to implement, it is likely to be reasonable for an organization to give its business associates time to implement such controls. The organization could continue to work with that business associate in the interim, but the absence of such controls would be a factor in the risk assessment and due diligence.

A.14 Anti-bribery commitments

A.14.1 This requirement to obtain anti-bribery commitments only applies in relation to business associates which pose more than a low bribery risk.

A.14.2 The risk of bribery in relation to a transaction is likely to be low, for example:

a) when the organization is purchasing a small number of very low value items;

c) when the organization is supplying low value goods or services direct to a customer (e.g. food, television etc.).

In these cases, the organization would not be required to obtain anti-bribery commitments from these low bribery risk suppliers or customers.

A.14.3 In the case of a business associate which poses a more than low bribery risk, then 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 therefore 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 sub-contractor 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.

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 benefits referred to in 8.7 could include, for example:

a) gifts, entertainment and hospitality;

b) political or charitable donations;

c) client or public official travel;

d) promotional expenses;

e) sponsorship;

f) community benefits;

g) training;

h) club memberships;

i) personal favours given in a business context.

A.15.2 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);

ii) frequency (relatively small gifts and hospitality can accumulate to a large amount if repeated);

iv) reasonableness (taking account of the location, sector and seniority of the giver or receiver);

v) identity of recipient (e.g. those in a position to award contracts or approve permits, certificates or payments);

vi) reciprocity (no-one in the organization can receive a gift or hospitality greater than a value which they are permitted to give);

vii) the legal and regulatory environment (some locations and organizations may have prohibitions or controls in place);

b) require approval in advance of gifts and hospitality above a defined value or frequency by an appropriate manager;

c) require gifts and hospitality above a defined value or frequency to be made openly, effectively documented (e.g. in a register, or accounts ledger), and supervised.

A.15.3 In relation to political or charitable donations, sponsorship, promotional expenses and community benefits the procedures implemented by the organization could, for example, be designed to:

a) prohibit payments which are intended to influence, or could reasonably be perceived to influence, a tender or other decision in favour of the organization;

b) undertake due diligence on the political party, charity or other recipient to ensure that they are legitimate and are not being used as a channel for bribery (this could include, for example, searches on the internet or other appropriate enquiries to ascertain whether the managers of the political party of charity have a reputation for bribery or similar criminal conduct, or are connected with the organization's projects or customers);

c) ensure that an appropriate manager approves the payment;

d) require public disclosure of the payment;

e) ensure that the payment is permitted by applicable law and regulations;

f) avoid making contributions during or immediately after contract negotiations.

A.15.4 In relation to client representative or public official travel, the procedures implemented by the organization could, for example, be designed to:

a) ensure that the payment is permitted by the procedures of the client or public body, and by applicable law and regulations;

b) ensure that the travel is necessary for the proper undertaking of the duties of the client representative or public official (e.g. to inspect the organization's quality procedures at its factory);

c) ensure that an appropriate manager of the organization approves the payment;

d) ensure if possible that the public official's supervisor or employer or anti-bribery compliance function is notified of the travel and hospitality to be provided;

e) restrict payments to the necessary travel, accommodation and meal expenses directly associated with a reasonable travel itinerary;

f) limit associated entertainment to a reasonable level as per the organization's gifts and hospitality policy;

g) prohibit paying the expenses of family members or friends;

h) prohibit the paying of holiday or recreational expenses.

of bribery even if neither the giver nor receiver intended it to be for this purpose. Therefore, 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.16 Internal audit

A.16.1 The requirement in 9.3 does not mean that an organization must 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 upon completion of the audit.

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).

i) the actions and outcomes of concerns raised in relation to:

   1) any weakness of the anti-bribery management system;

   2) incidents of attempted, suspected or actual bribery;

i) the results of monitoring, investigating or auditing carried out by the organization or third parties.

A.18.1 The standard requires the organization to implement appropriate procedures on how to investigate and deal with any issue of bribery, or breach of anti-bribery controls, which is reported, detected or reasonably suspected. How an organization investigates and deals with a particular issue will depend on the circumstances. Every situation is different, and the organization's response should be reasonable and proportionate to the circumstances. A report of a major issue of suspected bribery would require a far more urgent, significant and detailed action than a minor breach of anti-bribery controls. The suggestions below are for guidance only and should not be taken as prescriptive.

A.18.2 The compliance function should preferably be the recipient of any reports of suspected or actual bribery or breach of anti-bribery controls. If the reports go in the first instance to another person, then the organization's procedures should ensure that the report is passed on to the compliance function as soon as possible. In some cases, the compliance function will itself identify a suspicion or breach.

A.18.3 The procedure should determine who has responsibility for deciding how the issue is investigated and dealt with. For example:

a) a small organization may implement a procedure under which all issues, of whatever magnitude, should be reported straight away by the compliance function to top management for top management decision on how to respond;

b) a larger organization may implement a procedure under which:

   1) minor issues are dealt with by the compliance function, with a periodic summary report of all minor issues being made to top management;

   2) major issues are reported straight away by the compliance function to top management for top management decision on how to respond.

A.18.4 Upon identification of any issue, top management or the compliance function (as appropriate) should then assess the known facts and potential severity of the issue. If they do not already have sufficient facts on which to make a decision, they should commence an investigation.

A.18.5 The investigation should be carried out by a person who was not involved in the issue. It could be the compliance function, internal audit, another appropriate manager or an appropriate third party. The person investigating should be given appropriate authority, resources and access by top management to enable the investigation to be effectively carried out. The person investigating should preferably have had training or prior experience in conducting an investigation. The investigation should promptly establish the facts and collect all necessary evidence by, for example:

a) making enquiries to establish the facts;

b) collecting together all relevant documents and other evidence;

c) obtaining witness evidence;

d) where possible and reasonable, requesting reports on the issue to be made in writing and signed by the individuals making them.

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);

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, then organization should implement appropriate follow up actions. Depending on the circumstances and the severity of the issue, these could include one or more of:

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 compliance obligations;

d) effectiveness in addressing compliance failures previously identified; and

e) instances where internal compliance audits are not performed as scheduled.

Monitoring of compliance performance may include, for example, the following areas:

— noncompliance and 'near misses' (an incident without adverse effect);

— instances where compliance obligations are not met;

— instances where objectives are not achieved; and

— status of culture of compliance.

A.20 Public officials

The following list is not exhaustive and not all examples may apply in all jurisdictions. In assessing its anti-bribery risks, an organization should take into account the categories of public officials with which it deals or may deal, and seek legal advice in the case of any uncertainty.

The term public official can include the following:

a) public office holders at the national, state/provincial or municipal level, including members of legislative bodies, executive office holders and the judiciary;

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, such as the World Bank, United Nations, International Monetary Fund, etc.;

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[1)]

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.21 Anti-bribery initiatives

Although not a requirement of this International Standard, 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.

1) See Commentaries on the Convention on Combating Bribery of Foreign Public Officials In International Business Transactions, OECD, 21 November 1997.

Bibliography

[1] ISO 9000:2015 Quality management systems -- Fundamentals and vocabulary

[2] ISO 9001, Quality management systems. Requirements

[3] ISO 19011, Guidelines for auditing management systems

[4] ISO 14001, Environmental management systems. Requirements with guidance for use

[5] ISO 17000, Conformity assessment. Vocabulary and general principles

[6] ISO 19600, Compliance management systems. Guidelines

[7] ISO 22000, Food safety management systems. Requirements for any organization in the food chain

[8] ISO 26000, Guidance on social responsibility

[9] ISO 31000, Risk management. Principles and guidelines

[10] ISO/IEC Guide 73, Risk Management – Vocabulary

[11] ISO/IEC Guide 2, Standardization and related activities – General vocabulary

[12] BS 10500, Specification for an anti-bribery management system

Other publications

[13] UNITED NATIONS. United Nations Convention against Corruption. New York. 2004. (Available at: http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf)

[14] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Convention on the Bribery of Foreign Public Officials in International Business Transactions and Related Documents. Paris: OECD. 2010. (http://www.oecd.org/dataoecd/4/18/38028044.pdf)

Further reading

[15] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Good Practice Guidance on Internal Controls, Ethics, and Compliance. Paris: OECD. 2010.

[16] UNITED NATIONS GLOBAL COMPACT / TRANSPARENCY INTERNATIONAL. Reporting guidance on the 10th principle against corruption. UN Global Compact. 2009

[17] INTERNATIONAL CHAMBER OF COMMERCE, TRANSPARENCY INTERNATIONAL, UNITED NATIONS GLOBAL COMPACT AND WORLD ECONOMIC FORUM. RESIST: Resisting Extortion and Solicitation in International Transactions. A company tool for employee training. 2010.

[18] INTERNATIONAL CHAMBER OF COMMERCE, Rules on Combating Corruption, Paris: ICC.2011

[19] TRANSPARENCY INTERNATIONAL. Business Principles for Countering Bribery and associated tools. Berlin: Transparency International. 2013.

[20] TRANSPARENCY INTERNATIONAL. Corruption Perceptions Index

[21] TRANSPARENCY INTERNATIONAL. Bribe Payers Index.

[22] WORLD BANK. Worldwide Governance Indicators.

[23] INTERNATIONAL CORPORATE GOVERNANCE NETWORK. ICGN Statement and Guidance on Anti-Corruption Practices. London: ICGN. 2009.

[24] 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: World Economic Forum

[25] COMMITTEE OF THE SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

ICS 03.100.01

Price based on 43 pages