MALAYSIAN STANDARD

MS ISO 37001:2016

Anti-bribery management systems - Requirements with guidance for use (ISO 37001:2016, IDT) (Published by STANDARDS MALAYSIA in 2017)

ICS: 03.100.70, 03.100.01

Descriptors: management systems, anti-bribery, requirements, guidance for use

DEPARTMENT OF STANDARDS MALAYSIA

DEVELOPMENT OF MALAYSIAN STANDARDS

The **Department of Standards Malaysia (STANDARDS MALAYSIA)** is the national standards and accreditation body of Malaysia.

The main function of STANDARDS MALAYSIA is to foster and promote standards, standardisation and accreditation as a means of advancing the national economy, promoting industrial efficiency and development, benefiting the health and safety of the public, protecting the consumers, facilitating domestic and international trade and furthering international cooperation in relation to standards and standardisation.

Malaysian Standards (MS) are developed through consensus by committees which comprise balanced representation of producers, users, consumers and others with relevant interests, as may be appropriate to the subject at hand. To the greatest extent possible, Malaysian Standards are aligned to or are adoption of international standards. Approval of a standard as a Malaysian Standard is governed by the Standards of Malaysia Act 1996 [Act 549]. Malaysian Standards are reviewed periodically. The use of Malaysian Standards is voluntary except in so far as they are made mandatory by regulatory authorities by means of regulations, local by-laws or any other similar ways.

For the purposes of Malaysian Standards, the following definitions apply:

Revision: A process where existing Malaysian Standard is reviewed and updated which resulted in the publication of a new edition of the Malaysian Standard.

Confirmed MS: A Malaysian Standard that has been reviewed by the responsible committee and confirmed that its contents are current.

Amendment: A process where a provision(s) of existing Malaysian Standard is altered. The changes are indicated in an amendment page which is incorporated into the existing Malaysian Standard. Amendments can be of technical and/or editorial nature.

Technical corrigendum: A corrected reprint of the current edition which is issued to correct either a technical error or ambiguity in a Malaysian Standard inadvertently introduced either in drafting or in printing and which could lead to incorrect or unsafe application of the publication.

NOTE: Technical corrigenda are not to correct errors which can be assumed to have no consequences in the application of the MS, for example minor printing errors.

STANDARDS MALAYSIA has appointed **Malaysian Association of Standards Users** as the agent to develop, distribute and sell Malaysian Standards.

For further information on Malaysian Standards, please contact:

Department of Standards Malaysia
Ministry of Science, Technology and Innovation
Level 1 & 2, Block 2300, Century Square
Jalan Usahawan
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: 60 3 8318 0002
Fax: 60 3 8319 3131
http://www.jsm.gov.my
E-mail: central@jsm.gov.my

OR

Malaysian Association of Standards Users
(Company No. 1880-04-7)
No. 24 Jalan SS1/22A
Kampung Tunku
47300, Petaling Jaya
Selangor Darul Ehsan
MALAYSIA

Tel: 60 3 7876 2009
Fax: 60 3 7875 2168
http://www.standardsusers.org
E-mail: sda@standardsusers.org

Contents

		Page
Committee representation		iii
National foreword		iv
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Context of the organization	7
4.1	Understanding the organization and its context	7
4.2	Understanding the needs and expectations of stakeholders	8
4.3	Determining the scope of the anti-bribery management system	8
4.4	Anti-bribery management system	8
4.5	Bribery risk assessment	8
5	Leadership	9
5.1	Leadership and commitment	9
5.2	Anti-bribery policy	10
5.3	Organizational roles, responsibilities and authorities	11
6	Planning	12
6.1	Actions to address risks and opportunities	12
6.2	Anti-bribery objectives and planning to achieve them	13
7	Support	13
7.1	Resources	13
7.2	Competence	14
7.3	Awareness and training	15
7.4	Communication	16
7.5	Documented information	16

Contents *(continued)*

		Page
8	Operation	18
8.1	Operational planning and control	18
8.2	Due diligence	18
8.3	Financial controls	19
8.4	Non-financial controls	19
8.5	Implementation of anti-bribery controls by controlled organizations and by business associates	19
8.6	Anti-bribery commitments	20
8.7	Gifts, hospitality, donations and similar benefits	20
8.8	Managing inadequacy of anti-bribery controls	20
8.9	Raising concerns	20
8.10	Investigating and dealing with bribery	21
9	Performance evaluation	22
9.1	Monitoring, measurement, analysis and evaluation	22
9.2	Internal audit	22
9.3	Management review	23
9.4	Review by anti-bribery compliance function	24
10	Improvement	25
10.1	Nonconformity and corrective action	25
10.2	Continual improvement	26
Annex A	Guidance on the use of this document	27
Bibliography		54

Committee representation

The Industry Standards Committee on Organisational Management (ISC O) under whose authority this Malaysian Standard was adopted, comprises representatives from the following organisations:

Department of Social Welfare

Federation of Public Listed Companies

Malaysian Association of Standards Users (Secretariat)

Malaysian Employers Federation

Malaysian Institute of Corporate Governance

Malaysian International Chamber of Commerce and Industry

Ministry of Domestic Trade, Co-operative and Consumerism

Ministry of International Trade and Industry

National Archives of Malaysia

TM Research and Development Sdn Bhd

The Technical Committee on Anti-bribery Management System which recommended the adoption of the ISO Standard as Malaysian Standard consists of representatives from the following organisations:

Association of Certified Fraud Examiners

Construction Industry Development Board

Department of Standards Malaysia

Malaysian Administrative Modernisation and Management Planning Unit

Malaysian Anti-corruption Commission

Malaysian Institute of Corporate Governance

Malaysian International Chamber of Commerce and Industry

Master Builders Association Malaysia

Prime Minister's Department

The Institute of Internal Auditors Malaysia

The Malaysian Institute of Integrity

Transparency International Malaysia

National foreword

The adoption of the ISO Standard as a Malaysian Standard was recommended by the Technical Committee on Anti-bribery Management System under the authority of the Industry Standards Committee on Organisational Management.

This Malaysian Standard is identical with ISO 37001:2016, *Anti-bribery management systems - Requirements with guidance for use*, published by the International Organization for Standardization (ISO). However, for the purposes of this Malaysian Standard, the following apply:

a) in the source text, "this International Standard" should read "this Malaysian Standard";

b) the comma which is used as a decimal sign (if any), to read as a point; and

c) in the Biobliography, reference to International Standards should be replaced by equivalent Malaysian Standards as follows:

Referenced International Standards	Corresponding Malaysian Standards
ISO 9000, *Quality management systems - Fundamentals and vocabulary*	MS ISO 9000, *Quality management systems - Fundamentals and vocabulary*
ISO 9001, *Quality management systems - Requirements*	MS ISO 9001, *Quality management systems - Requirements*
ISO 19011, *Guidelines for auditing management systems*	MS ISO 19011, *Guidelines for auditing management systems*
ISO 14001, *Environmental management systems - Requirements with guidance for use*	MS ISO 14001, *Environmental management systems - Requirements with guidance for use*
ISO/IEC 17000, *Conformity assessment - Vocabulary and general principles*	MS ISO/IEC 17000, *Conformity assessment - Vocabulary and general principles*
ISO 22000, *Food safety management systems - Requirements for any organization in the food chain*	MS ISO 22000, *Food safety management systems - Requirements for any organization in the food chain*
ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*	MS ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*
ISO 31000, *Risk management - Principles and guidelines*	MS ISO 31000, *Risk management - Principles and guidelines*
ISO Guide 73, *Risk management - Vocabulary*	MS ISO Guide 73, *Risk management - Vocabulary*

National foreword *(continued)*

Compliance with a Malaysian Standard does not of itself confer immunity from legal obligations.

NOTE. IDT on the front cover indicates an identical standard i.e. a standard where the technical content, structure, and wording (or is an identical translation) of a Malaysian Standard is exactly the same as in an International Standard or is identical in technical content and structure although it may contain the minimal editorial changes specified in clause 4.2 of ISO/IEC Guide 21-1.

Introduction

Bribery is a widespread phenomenon. It raises serious social, 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 can 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 Convention on Combating Bribery of Foreign Public Officials in International Business Transactions[15] and the United Nations Convention against Corruption[14] 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.

However, the law alone is not sufficient to solve this problem. Organizations have a responsibility to proactively contribute to combating bribery. This can be achieved by an anti-bribery management system, which this document is intended to provide, and 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.

A well-managed organization is expected to 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 document reflects international good practice and can be used in 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. This document 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 document.

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

In this document, the following verbal forms are used:

— "shall" indicates a requirement;

— "should" indicates a recommendation;

— "may" indicates a permission;

— "can" indicates a possibility or a capability.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirement.

This document conforms to ISO's requirements for management system standards. These requirements include a high level structure, identical core text, and common terms with core definitions, designed to benefit users implementing multiple ISO management system standards. This document can be used in conjunction with other management system standards (e.g. ISO 9001, ISO 14001, ISO/IEC 27001 and ISO 19600) and management standards (e.g. ISO 26000 and ISO 31000).

Anti-bribery management systems - Requirements with guidance for use

1 Scope

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

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; and

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

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

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

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

NOTES:

1. See Clause A.2 for guidance.

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

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at http://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1 bribery

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* (3.16) of that person's duties.

Note 1 to entry: The above is a generic definition. The meaning of the term "bribery" is as defined by the anti-bribery law applicable to the *organization* (3.2) and by the anti-bribery *management system* (3.5) designed by the organization.

3.2 organization

Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (3.11).

Notes to entry:

1. 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.

2. For organizations with more than one operating unit, one or more of the operating units can be defined as an organization.

3.3 interested party (preferred term), stakeholder (admitted term)

Person or *organization* (3.2) 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.

3.4 requirement

Need that is stated and obligatory.

Notes to entry:

1. The core definition of "requirement" in ISO management system standards is "need or expectation that is stated, generally implied or obligatory". "Generally implied requirements" are not applicable in the context of anti-bribery management.

2. "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

3. A specified requirement is one that is stated, for example in documented information.

3.5 management system

Set of interrelated or interacting elements of an *organization* (3.2) to establish *policies* (3.10) and *objectives* (3.11) and *processes* (3.15) to achieve those objectives.

Notes to entry:

1. A management system can address a single discipline or several disciplines.

2. The management system elements include the organization's structure, roles and responsibilities, planning and operation.

3. 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.

3.6 top management

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

Notes to entry:

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

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

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

3.7 governing body

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

Notes to entry:

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

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

3.8 anti-bribery compliance function

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

3.9 effectiveness

Extent to which planned activities are realized and planned results achieved.

3.10 policy

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

3.11 objective

Result to be achieved.

Notes to entry:

1. An objective can be strategic, tactical or operational.

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

3. 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).

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

3.12 risk

Effect of uncertainty on objectives (3.11).

Notes to entry:

1. An effect is a deviation from the expected — positive or negative.

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

3. 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.

4. 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.

3.13 competence

Ability to apply knowledge and skills to achieve intended results.

3.14 documented information

Information required to be controlled and maintained by an *organization* (3.2) and the medium on which it is contained.

Notes to entry:

1. Documented information can be in any format and media, and from any source.

2. Documented information can refer to:

- the *management system* (3.5), including related *processes* (3.15);
- information created in order for the organization to operate (documentation);
- evidence of results achieved (records).

3.15 process

Set of interrelated or interacting activities which transforms inputs into outputs.

3.16 performance

Measurable result.

Notes to entry:

1. Performance can relate either to quantitative or qualitative findings.

2. Performance can relate to the management of activities, *processes* (3.15), products (including services), systems or *organizations* (3.2).

3.17 outsource (verb)

Make an arrangement where an external *organization* (3.2) performs part of an organization's function or *process* (3.14).

Notes to entry:

1. An external organization is outside the scope of the *management system* (3.5), although the outsourced function or process is within the scope.

2. The core text of ISO management system standards contains a definition and requirement in relation to outsourcing, which is not used in this document, as outsourcing providers are included within the definition of business associate (3.26).

3.18 monitoring

Determining the status of a system, a *process* (3.15) or an activity.

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

3.19 measurement

Process (3.15) to determine a value.

3.20 audit

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

Notes to entry:

1. 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).

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

3. "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.21 conformity

Fulfilment of a *requirement* (3.4).

3.22 nonconformity

Non-fulfilment of a *requirement* (3.4).

3.23 corrective action

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

3.24 continual improvement

Recurring activity to enhance *performance* (3.16).

3.25 personnel

Organization's (3.2) directors, officers, employees, temporary staff or workers, and volunteers.

Notes to entry:

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

2. See A.8.5 for guidance on temporary staff or workers.

3.26 business associate

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

Notes to entry:

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

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

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

3.27 public official

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

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

3.28 third party

Person or body that is independent of the *organization* (3.2).

Note 1 to entry: All *business associates* (3.26) are third parties, but not all third parties are business associates.

3.29 conflict of interest

Situation where business, financial, family, political or personal interests could interfere with the judgment of persons in carrying out their duties for the *organization* (3.2).

3.30 due diligence

Process (3.15) to further assess the nature and extent of the bribery *risk* (3.12) and help *organizations* (3.2) make decisions in relation to specific transactions, projects, activities, *business associates* (3.26) and personnel.

4 Context of the organization

4.1 Understanding the organization and its context

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

a) the size, structure and delegated decision-making authority of the organization;

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

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

d) the organization's business model;

e) the entities over which the organization has control and entities which exercise control over the organization;

f) the organization's business associates;

g) the nature and extent of interactions with public officials;

h) 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 (see A.13.1.3).

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 issues referred to in 4.1;

b) the requirements referred to in 4.2;

c) the results of the bribery risk assessment referred to in 4.5.

The scope shall be available as documented information.

NOTE. See Clause A.2 for guidance.

4.4 Anti-bribery management system

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

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

NOTES:

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.

2. See Clause A.3 for guidance.

4.5 Bribery risk assessment

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

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

b) analyse, assess and prioritize the identified bribery risks;

c) evaluate the suitability and effectiveness of the organization's existing controls to mitigate the assessed bribery risks.

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

4.5.3 The bribery risk assessment shall be reviewed:

a) on a regular basis so that changes and new information can be properly assessed based on timing and frequency defined by the organization;

b) in the event of a significant change to the structure or activities of the organization.

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

NOTE. See Clause A.4 for guidance.

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) ensuring that the organization's strategy and anti-bribery policy are aligned;

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

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

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

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;

i) promoting continual improvement;

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 8.9);

l) ensuring that no personnel will suffer retaliation, discrimination or disciplinary action [see 7.2.2.1 d)] for reports made in good faith, or on the basis of a reasonable belief of violation or suspected violation of the organization's anti-bribery policy, or for refusing to engage in bribery, even if such refusal can result in the organization losing business (except where the individual participated in the violation);

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

NOTE. See Clause A.5 for guidance.

5.2 Anti-bribery policy

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

a) prohibits bribery;

b) requires compliance with anti-bribery laws that are applicable to the organization;

c) is appropriate to the purpose of the organization;

d) provides a framework for setting, reviewing and achieving anti-bribery objectives;

e) includes a commitment to satisfy anti-bribery management system requirements;

f) encourages raising concerns in good faith, or on the basis of a reasonable belief in confidence, without fear of reprisal;

g) includes a commitment to continual improvement of the anti-bribery management system;

h) explains the authority and independence of the anti-bribery compliance function;

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

The anti-bribery policy shall:

— be available as documented information;

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

— be available to relevant stakeholders, as appropriate.

5.3 Organizational roles, responsibilities and authorities

5.3.1 Roles and responsibilities

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

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

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

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

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 document; and

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, authority 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 can 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 externally assigned parts of the function.

NOTE. See Clause A.6 for guidance.

5.3.3 Delegated decision-making

Where top management delegates to personnel the 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 which 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 role and responsibility for implementation of, and compliance with, the anti-bribery management system outlined in 5.3.1.

NOTE. Delegation of decision-making does not exempt top management or the governing body (if any) of their duties and responsibilities as described in 5.1.1, 5.1.2 and 5.3.1, nor does it necessarily transfer to the delegated personnel potential legal responsibilities.

6 Planning

6.1 Actions to address risks and opportunities

When planning for the anti-bribery management system, the organization shall consider the issues referred to in 4.1, the requirements referred to in 4.2, the risks identified in 4.5, and opportunities for improvement 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;

d) achieve continual improvement.

The organization shall plan:

— actions to address these bribery risks and opportunities for improvement;

— how to:

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

- evaluate the effectiveness of these actions.

6.2 Anti-bribery objectives and planning to achieve them

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

The anti-bribery management system objectives shall:

a) be consistent with the anti-bribery policy;

b) be measurable (if practicable);

c) take into account applicable factors referred to in 4.1, the requirements referred to in 4.2 and the bribery risks identified in 4.5;

d) be achievable;

e) be monitored;

f) be communicated in accordance with 7.4;

g) be updated as appropriate.

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

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

— what will be done;

— what resources will be required;

— who will be responsible;

— when the objectives will be achieved;

— how the results will be evaluated and reported;

— who will impose sanctions or penalties.

7 Support

7.1 Resources

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

NOTE. See Clause A.7 for guidance.

7.2 Competence

7.2.1 General

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 the same.

7.2.2 Employment process

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 violate the anti-bribery policy or anti-bribery management system;

d) personnel will not suffer retaliation, discrimination or disciplinary action (e.g. by threats, isolation, demotion, preventing advancement, transfer, dismissal, bullying, victimization, or other forms of harassment) for:

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

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

7.2.2.2 In relation to all positions which are exposed to more than a low bribery risk, as determined in the bribery risk assessment (see 4.5), and to 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, 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.

NOTES:

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

2. See Clause A.8 for guidance.

7.3 Awareness and training

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

a) the organization's anti-bribery policy, procedures and anti-bribery management system, and their duty to comply;

b) the bribery risk and the damage to them and the organization which can result from bribery;

c) the circumstances in which bribery can occur in relation to their duties, and how to recognize these circumstances;

d) how to recognize and respond to solicitations or offers of bribes;

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

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

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

h) how and to whom they are able to report any concerns (see 8.9);

i) information on available training and resources.

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

Taking into account the bribery risks identified (see 4.5), the organization shall also implement procedures addressing anti-bribery awareness and training for business associates acting on

its behalf or for its benefit, and which could pose more than a low bribery risk to the organization. These procedures shall identify the business associates for which such awareness and training is necessary, its content, and the means by which the training shall be provided.

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

NOTES:

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

2. See Clause A.9 for guidance.

7.4 Communication

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

a) on what it will communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate;

e) who will 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 document;

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

NOTES:

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.

2. Documented information can be retained separately as part of the anti-bribery management system, or can be retained as part of other management systems (e.g. compliance, financial, commercial, audit).

3. See Clause 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 document 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);

— retention and disposition.

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

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

8 Operation

8.1 Operational planning and control

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

a) establishing criteria for the processes;

b) implementing control of the processes in accordance with the criteria;

c) keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

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

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

The organization shall ensure that outsourced processes are controlled.

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

8.2 Due diligence

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

a) specific categories of transactions, projects or activities,

b) planned or on-going relationships with specific categories of business associates, or

c) specific categories of personnel in certain positions (see 7.2.2.2),

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

NOTES:

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

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

3. See Clause A.10 for guidance.

8.3 Financial controls

The organization shall implement financial controls that manage bribery risk.

NOTE. See Clause A.11 for guidance.

8.4 Non-financial controls

The organization shall implement non-financial controls that manage bribery risk with respect to such areas as procurement, operational, sales, commercial, human resources, legal and regulatory activities.

NOTES:

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

2. See Clause 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 with regard to the bribery risks faced by the controlled organizations, taking into account the bribery risk assessment conducted in accordance with 4.5.

NOTE. An organization has control over another organization if it directly or indirectly controls the management of the organization (see A.13.1.3).

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) where practicable, the organization shall 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, this shall be a factor taken into account in evaluating the bribery risk of the relationship with this business associate (see 4.5 and 8.2) and the way in which the organization manages such risks (see 8.3, 8.4 and 8.5).

NOTE. See Clause A.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 practicable:

a) business associates commit to preventing bribery by, on behalf of, or for the benefit of the business associate in connection with the relevant transaction, project, activity, or relationship;

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

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

NOTE. See Clause A.14 for guidance.

8.7 Gifts, hospitality, donations and similar benefits

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

NOTE. See Clause A.15 for guidance.

8.8 Managing inadequacy of anti-bribery controls

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

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

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

8.9 Raising concerns

The organization shall implement procedures which:

a) encourage and enable persons to report in good faith or on the basis of a reasonable belief attempted, suspected and actual bribery, or any violation of or weakness in the anti-bribery management system, to the anti-bribery compliance function or to appropriate personnel (either directly or through an appropriate third party);

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

c) allow anonymous reporting;

d) prohibit retaliation, and protect those making reports from retaliation, after they have in good faith, or on the basis of a reasonable belief, raised or reported a concern about attempted, actual or suspected bribery or violation of the anti-bribery policy or the anti-bribery management system;

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

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

NOTES:

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

2. The organization can use a business associate to manage the reporting system on its behalf.

3. In some jurisdictions, the requirements in b) and c) above are prohibited by law. In these cases, the organization documents its inability to comply.

8.10 Investigating and dealing with bribery

The organization shall implement procedures that:

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

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

c) empower and enable investigators;

d) require co-operation in the investigation by relevant personnel;

e) require that the status and results of the investigation are reported to the anti-bribery compliance function and other compliance functions, as appropriate;

f) require that the investigation is carried out confidentially and that the outputs of the investigation are confidential.

The investigation shall be carried out by, and reported to, personnel who are not part of the role or function being investigated. The organization can appoint a business associate to conduct the investigation and report the results to personnel who are not part of the role or function being investigated.

NOTES:

1. See Clause A.18 for guidance.

2. In some jurisdictions, the requirement in f) above is prohibited by law. In this case, the organization documents its inability to comply.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured;

b) who is responsible for monitoring;

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

d) when the monitoring and measuring shall be performed;

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

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

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

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

NOTE. See Clause A.19 for guidance.

9.2 Internal audit

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

a) conforms to:

   1) the organization's own requirements for its anti-bribery management system;

   2) the requirements of this document;

b) is effectively implemented and maintained.

NOTES:

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

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

9.2.2 The organization shall:

a) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits;

b) define the audit criteria and scope for each audit;

c) select competent auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

d) ensure that the results of the audits are reported to relevant management, the anti-bribery compliance function, top management and, as appropriate, the governing body (if any);

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

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

a) bribery or suspected bribery;

b) violation of the anti-bribery policy or anti-bribery management system requirements;

c) failure of business associates to conform to the applicable anti-bribery requirements of the organization;

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

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

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

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 Clause A.16 for guidance.

9.3 Management review

9.3.1 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:

a) the status of actions from previous management reviews;

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

c) information on the performance of the anti-bribery management 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;

d) effectiveness of actions taken to address bribery risks;

e) 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 (if any).

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

9.3.2 Governing body review

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

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

9.4 Review by anti-bribery compliance function

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

a) adequate to manage effectively the bribery risks faced by the organization;

b) being effectively implemented.

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

Notes:

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

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

10 Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react promptly to the nonconformity, and as applicable:

   1) take action to control and correct it;

   2) deal with the consequences;

b) evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by:

   1) reviewing the nonconformity;

   2) determining the causes of the nonconformity;

   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the anti-bribery management system, if necessary.

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

The organization shall retain documented information as evidence of:

— the nature of the nonconformities and any subsequent actions taken;

— the results of any corrective action.

NOTE. See Clause A.20 for guidance.

10.2 Continual improvement

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

NOTE. See Clause A.20 for guidance.

Annex A
(informative)

Guidance on the use of this document

A.1 General

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

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

A.2 Scope of the anti-bribery management system

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

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

A.2.2 Facilitation and extortion payments

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

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

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

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

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;

2) reporting the event to an appropriate manager or the anti-bribery compliance function;

c) 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 respond to. Recognizing these difficulties, the overall intent of this document is that the governing body (if any) and top management of an organization need to:

— have a genuine commitment to prevent, detect and respond to bribery in relation to the organization's business or activities;

— with genuine intent, implement measures in the organization that are designed to prevent, detect and respond to 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 occur. 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 responding to bribery.

A.3.2 While the types of anti-bribery measures that need to be implemented are reasonably well recognized by international good practice, and some of which are reflected as requirements in this document, the detail of the measures to be implemented differ widely according to the

relevant circumstances. It is impossible to prescribe in detail what an organization should do in any particular circumstance. The "reasonable and proportionate" qualification has been introduced into this document, 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 can apply in relation to differing circumstances.

a) A very large multi-national organization could need to deal with multiple layers of management, and thousands of personnel. Its anti-bribery management system will 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 many transactions or activities, the bribery risk assessment, due diligence procedures and anti-bribery controls implemented by an organization involved in a large, high value transaction or activities involving a wide range of business associates are likely to be more comprehensive than those implemented by an organization in relation to a business which involves selling small value items to multiple customers or multiple smaller transactions with a single party.

d) An organization with a very broad range of business associates can conclude, as part of its bribery risk assessment, that certain categories of business associates, e.g. retail customers, are unlikely to pose more than a low bribery risk, and take that into account in the design and implementation of its anti-bribery management system. For example, due diligence is unlikely to be necessary, or to be a proportionate and reasonable control, in relation to retail customers who are purchasing items such as consumer goods from the organization.

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

A.4 Bribery risk assessment

A.4.1 The intention of the bribery risk assessment required by 4.5 is to enable the organization to form a solid foundation for its anti-bribery management system. This assessment identifies the bribery risks that the management system will focus on, i.e. the bribery risks deemed by the organization to be a priority for bribery risk mitigation, control implementation and allocation of anti-bribery compliance personnel, resources and activities.

How the organization undertakes the bribery risk assessment, what methodology it employs, how the bribery risks are weighted and prioritized, and the level of bribery risk that is accepted (i.e. "risk appetite") or tolerated, are all at the discretion of the organization. In particular, it is

the organization that establishes its criteria for evaluating bribery risk (e.g. whether a risk is "low", "medium" or "high"); however, in so doing, the organization should take into account its anti-bribery policy and objectives.

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

a) Select bribery risk evaluation criteria. For example, the organization can select three-tier criteria (e.g. "low", "medium", "high"), more detailed five-level or seven-level criteria, or a more detailed approach. The criteria will often take into account several factors, including the nature of the bribery risk, the likelihood of bribery occurring, and the magnitude of the consequences should it occur.

b) Assess the bribery risks posed by the size and structure of the organization. A small organization based in one location with centralized management controls in the hands of a few people may be able to control its bribery risk more easily than a very large organization with a decentralized structure operating in many locations.

c) Examine the locations and sectors in which the organization operates or anticipates operating, and assess the level of bribery risk these locations and sectors can pose. An appropriate bribery index can be used to assist in this assessment. Locations or sectors with a higher risk of bribery can be deemed by the organization as "medium" or "high" risk, for example, which can result in the organization imposing a higher level of controls applicable to activities by the organization in those locations or sectors.

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

   1) It can 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 can carry specific bribery risks, e.g. offset arrangements by which the government 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 prevent the offset arrangements from constituting 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 can have large numbers of customers that purchase very low value products from the organization and that in practice pose a minimal bribery risk to the organization. In this case the organization may deem these customers low bribery risk, and can determine that these customers will not need to have any specific anti-bribery controls related to them. Alternatively, the organization can deal with customers which buy very large value products from the organization, and can pose a significant bribery risk (e.g. the risk of demanding bribes from the organization in return for payments, approvals). These types of customers can be deemed as "medium" or "high" bribery risk, and they can 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 which could be in contact with the organization's clients, customers or relevant public officials, can 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 of suppliers can pose a "very low" bribery risk, e.g. suppliers of low quantities of low value items, online purchasing services for air travel or hotels. The organization might conclude that specific anti-bribery controls do not need to be implemented in relation to these low or very low bribery risk 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.

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

g) Examine applicable statutory, regulatory, contractual and professional obligations and duties, e.g. 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 can 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 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 can 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 document 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 can change the nature of the transaction, project, activity or relationship such that the nature and extent of the bribery risk is reduced to a level that can be adequately managed by existing, enhanced or additional anti-bribery controls.

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

NOTE. Further guidance is given in ISO 31000.

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

A.5.1 Many organizations have some form of governing body (e.g. a board of directors or

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

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

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

A.6 Anti-bribery compliance function

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

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

a) "competence" means that the relevant person(s) has the appropriate education, training or experience, 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 can be exposed to bribery while performing their primary function. In the case of a very small organization where it can 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 to the governing body (if any), 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 any), 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 is given in ISO 19600.

A.7 Resources

Resources needed depend on factors such as the size of the organization, the nature of its operations, and the bribery risks it faces. Examples of resources include the following.

a) **Human resources:** There should be sufficient personnel who 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:** There should be the necessary physical resources in the organization, including in the anti-bribery compliance function, for the anti-bribery management system to function effectively, e.g. office space, furniture, computer hardware and software, training materials, telephones, stationery.

c) **Financial resources:** There should be a sufficient budget, including in the anti-bribery compliance function, for the anti-bribery management system to 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, can take actions such as:

a) discussing the organization's anti-bribery policy with prospective personnel at interview, and forming a view as to whether they appear to understand and accept the importance of compliance;

b) taking reasonable steps to verify that prospective personnel's qualifications are accurate;

c) taking reasonable steps to obtain satisfactory references from prospective personnel's previous employers;

d) taking reasonable steps to determine whether prospective personnel have been involved in bribery;

e) taking reasonable steps to verify that the organization is not offering employment to prospective personnel in return for their having, in previous employment, improperly favoured the organization;

f) verifying that the purpose of offering employment to prospective personnel is not to secure improper favourable treatment for the organization;

g) taking reasonable steps to identify the prospective personnel's relationship to public officials.

A.8.2 Performance bonuses

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

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

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

A.8.3 Conflicts of interest

The organization should identify and evaluate the risk of internal and external conflicts of interest. The organization should clearly inform all personnel of their duty to report any actual

or potential conflict of interest such as family, financial or other connection directly or indirectly related to their line of work. This helps an organization to identify situations where personnel may facilitate or fail to prevent or report bribery, e.g.

a) when the organization's sales manager is related to a customer's procurement manager, or

b) when an organization's line manager has a personal financial interest in a competitor's business.

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

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 may 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 and permits). As the bribe is likely to be accepted by personnel outside of the scope of the organization's systems or 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 document dealing with this risk:

a) the organization's anti-bribery policy (see 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 (see 7.3) should reinforce the prohibition on soliciting and accepting bribes, and include:

   1) guidance for reporting bribery concerns (see 8.9);

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

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

d) the publication on the organization's website of the organization's anti-bribery policy and of details of how to report bribery 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 (see 8.3 and 8.4) requiring, for example, the use of approved suppliers, competitive bidding, at least two signatures on contract awards, work approvals, etc. reduce the risk of corrupt awards, approvals, payments or benefits.

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 business expense records to identify unusual spending;

c) comparing personnel payroll file information (e.g. personal bank account numbers and addresses) with the bank account and address information in the organization's vendor master file to identify potential conflict of interest scenarios.

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 business associate. 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 business associate which provides the temporary staff or workers.

A.9 Awareness and training

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

a) the bribery risks they and their organization face;

b) the anti-bribery policy;

c) the aspects of the anti-bribery management system relevant to their role;

d) any necessary preventive and reporting actions they need to take in relation to any bribery risk or suspected bribery.

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

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

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

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

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

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

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

The organization can communicate these obligations to its business associates in a variety of ways, including as part of contractual arrangements.

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 (see 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 In relation to projects, transactions and activities, factors that the organization may find useful to evaluate include:

a) structure, nature and complexity (e.g. direct or indirect sale, level of discount, contract award and tender procedures);

b) financing and payment arrangements;

c) scope of the organization's engagement and available resources;

d) level of control and visibility;

e) business associates and other third parties involved (including public officials);

f) links between any parties in e) above and public officials;

g) competence and qualifications of the parties involved;

h) client's reputation;

i) location;

j) reports in the market or in the press.

A.10.3 In relation to possible due diligence on business associates:

a) factors which the organization may find useful to evaluate in relation to a business associate include:

1) 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;

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

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

4) 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;

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

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

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

iii) have any direct or indirect links to the organization's customer or client or to a relevant public official which could lead to bribery (this would include persons who are not public officials themselves, but who may be directly or indirectly related to public officials, candidates for public office, etc.);

6) the structure of the transaction and payment arrangements;

b) the nature, type and extent of due diligence undertaken will depend on factors such as the ability of the organization to obtain sufficient information, the cost of obtaining information, and the extent of the possible bribery risk posed by the relationship;

c) the due diligence procedures implemented by the organization on its business associates should be consistent across similar bribery risk levels (high bribery risk business associates in locations or markets where there is a high risk of bribery are likely to require a significantly higher level of due diligence than lower bribery risk business associates in low bribery risk locations or markets);

d) different types of business associates are likely to require different levels of due diligence, for example:

1) from the perspective of the organization's potential legal and financial liability, business associates pose a higher bribery risk to the organization when they are acting on the organization's behalf or for its benefit than when they are providing products or services to the organization. For example, an agent involved in assisting an organization to obtain a contract award could pay a bribe to a manager of the organization's customer to help the organization win the contract, and so could result in the organization being responsible for the agent's corrupt conduct. As a result, the organization's due diligence on the agent is likely to be as comprehensive as possible. On the other hand, a supplier selling equipment or material to the organization and which has no involvement with the organization's customers or public officials that are relevant to the organization's activities is less likely to be able to pay a bribe on the organization's behalf or for its benefit, and so the level of due diligence on the supplier could be lower;

2) the level of influence which the organization has over its business associates also affects the organization's ability to obtain information directly from those business associates as part of its due diligence. It may be relatively easy for an organization to require its agents and joint venture partners to provide extensive information about themselves as part of a due diligence exercise prior to the organization committing to work with them, as the organization has a degree of choice over with whom it contracts in this situation. However, it may be more difficult for an organization to require a customer or client to provide information about themselves or to fill in due diligence questionnaires. This could be because the organization would not have sufficient influence over the client or customer to be able to do so (for example where the organization is involved in a competitive tender to provide services to the customer);

e) the due diligence undertaken by the organization on its business associates may include, for example:

1) a questionnaire sent to the business associate in which it is asked to answer the questions referred to in A.10.3 a);

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

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

4) checking publicly available debarment lists of organizations that are restricted or prohibited from contracting with public or government entities kept by national or local governments or multilateral institutions, such as the World Bank;

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

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

f) the business associate can be asked further questions based on the results of the initial due diligence (e.g. to explain any adverse information).

A.10.4 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.10.5 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) verifying that the payee's appointment and work or services carried out have been approved by the organization's relevant approval mechanisms;

d) requiring at least two signatures on payment approvals;

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) requiring 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 that 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 the procurement, operational, commercial and other non-financial aspects of its activities 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, the following controls:

a) using approved contractors, 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 Clause 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;

3) whether any payments to be made to the business associate are reasonable and proportionate with regard to those services. This is particularly important in order to avoid the risk that the business associate uses part of the payment made to it by the organization to pay a bribe on behalf of or for the benefit of the organization. For example, if an agent has been appointed by the organization to assist with sales and is to be paid a commission or a contingency fee on award of a contract to the organization, the organization needs to be reasonably satisfied that the commission payment is reasonable and proportionate with regard to the legitimate services actually carried out by the agent, taking into account the risk assumed by the agent in case the contract is not awarded. If a disproportionately large commission or contingency fee is paid, there is an increased risk that part of it could be improperly used by the agent to induce a public official or an employee of the organization's client to award the contract to the organization. The organization may also request that its business associates provide documentation that demonstrates that the services have been provided;

c) awarding contracts, where possible and reasonable, only after a fair and, where appropriate, transparent competitive tender process between at least three competitors has taken place;

d) requiring at least two persons to evaluate the tenders and approve the award of a contract;

e) implementing a separation of duties, so that personnel who approve the placement of a contract are different from those requesting the placement of the contract and are from a different department or function from those who manage the contract or approve work done under the contract;

f) requiring the signatures of at least two persons on contracts, and on documents which change the terms of a contract or which approve work undertaken or supplies provided under the contract;

g) placing a higher level of management oversight on potentially high bribery risk transactions;

h) protecting the integrity of tenders and other price-sensitive information by restricting access to appropriate people;

i) providing appropriate tools and templates to assist personnel (e.g. practical guidance, do's and don'ts, approval ladders, checklists, forms, IT workflows).

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

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

A.13.1 General

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

a) a subsidiary of the organization paying a bribe with the result that the organization can be liable;

b) a joint venture or joint venture partner paying a bribe to win work for a joint venture in which the organization participates;

c) a procurement manager of a customer or client demanding a bribe from the organization in return for a contract award;

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, 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 require 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 itself, or by the controlled organization implementing its own specific anti-bribery controls. These controls should be reasonable and proportionate with regard to the bribery risks which the controlled organization faces, taking into account the bribery risk assessment conducted in accordance with 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), that controlled business associate would fall under the requirements in 8.5.1.

A.13.3 Non-controlled business associates

A.13.3.1 In respect of business associates that are not controlled by the organization, the organization may not need to take the steps required by 8.5.2 to require implementation by the business associate of anti-bribery controls in the following circumstances:

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).

This reflects the reasonableness and proportionality of this document.

A.13.3.2 If the bribery risk assessment (see 4.5) or due diligence (see 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, the organization should take the following further steps under 8.5.

a) The organization determines whether the business associate has in place appropriate anti-bribery controls which manage the relevant bribery risk. The organization should make this determination after undertaking appropriate due diligence (see Clause A.10). The organization is trying to verify that these controls manage the bribery risk relevant to the transaction between the organization and the business associate. The organization does not need to verify that the business associate has controls over its wider bribery risks. Note that both the extent of the controls and the steps that the organization needs to take to verify these controls should be reasonable and proportionate to the relevant bribery risk. If the organization has determined as far as it reasonably can that the business associate does have in place appropriate controls, the requirement of 8.5 is addressed in relation to that business associate. See A.13.3.4 for comments on appropriate types of controls.

b) If the organization identifies that the business associate does not have in place appropriate anti-bribery controls that manage the relevant bribery risks, or if it is not possible to verify whether it has these controls in place, the organization undertakes the following further steps.

1) If it is practicable (see A.13.3.3) to do so, the organization requires the business associate to implement anti-bribery controls (see A.13.3.4) in relation to the relevant transaction, project or activity.

2) Where it is not practicable (see A.13.3.3) to require the business associate to implement anti-bribery controls, the organization takes this factor into account when assessing the bribery risks that the business associate poses, and the way in which the organization manages such risks. This does not mean that the organization cannot go ahead with the relationship or transaction. However, the organization should consider, as part of the bribery risk assessment, the likelihood of the business associate being involved in bribery, and the organization should take the absence of such controls into account in assessing the overall bribery risk. If the organization believes that the bribery risks posed by this business associate are unacceptably high, and the bribery risk cannot be reduced by other means (e.g. re-structuring the transaction), the provisions of 8.8 will apply.

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

a) It will normally be practicable when the organization has a significant degree of influence over the business associate. For example, where the organization is appointing an agent to act on its behalf in a transaction, or is appointing a sub-contractor with a large scope of work. In this case, the organization will normally be able to make implementation of anti-bribery controls a condition of appointment.

b) It will normally not be practicable when the organization does not have a significant degree of influence over the business associate, e.g.

1) a client for a project;

2) a specific sub-contractor or supplier nominated by the client;

3) a major sub-contractor or supplier when the bargaining power of the supplier or sub-contractor is far greater than that of the organization (e.g. when the organization is buying components from a major supplier on the supplier's standard terms).

c) It will normally not be practicable when the business associate lacks the resources or expertise to be able to implement controls.

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

a) In the case of a 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 document 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, e.g. 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 can implement monitoring, reporting and/or audit procedures.

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 undertaken. However, the organization should consider requiring a right to terminate the relevant contract or agreement if the business associate does not effectively implement the required controls in a timely manner.

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;

b) when the organization is booking air tickets or hotel rooms online direct from the airlines or hotels;

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

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, the organization should, where practicable, obtain anti-bribery commitments from that business associate.

a) It will normally be practicable to require these commitments when the organization has influence over the business associate and it can insist on the business associate giving these commitments. The organization is likely to be able to require these commitments, for example, where the organization is appointing an agent to act on its behalf in a transaction, or is appointing a 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 undertaken under 4.5 and 8.2.

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

A.15 Gifts, hospitality, donations and similar benefits

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

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

a) gifts, entertainment and hospitality;

b) political or charitable donations;

c) client representative or public official travel;

d) promotional expenses;

e) sponsorship;

f) community benefits;

g) training;

h) club memberships;

i) personal favours;

j) confidential and privileged information.

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

a) control the extent and frequency of gifts and hospitality by:

1) a total prohibition on all gifts and hospitality; or

2) permitting gifts and hospitality, but limiting them by reference to such factors as:

   i) a maximum expenditure (which may vary according to the location and the type of gift and hospitality);

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

   iii) timing (e.g. not during or immediately before or after tender negotiations);

   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.15.4 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 determine whether they are legitimate and are not being used as a channel for bribery (e.g. this could include searches on the internet or other appropriate enquiries to ascertain whether the managers of the political party or charity have a reputation for bribery or similar criminal conduct, or are connected with the organization's projects or customers);

c) require 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 immediately before, during or immediately after contract negotiations.

A.15.5 In relation to client representative or public official travel, the procedures

implemented by the organization could, for example, be designed to:

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

b) only allow travel that 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) require that an appropriate manager of the organization approves the payment;

d) require 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.

A.16 Internal audit

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

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

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

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

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

A.16.6 The intention of the audit is to provide reasonable assurance to the governing body (if any) and top management that the anti-bribery management system has been implemented and is operating effectively, to help prevent and detect bribery, and to provide a deterrent to

any potentially corrupt personnel (as they will be aware that their project or department could be selected for audit).

A.17 Documented information

The documented information under 7.5.1 may include:

a) receipt of anti-bribery policy by personnel;

b) provision of anti-bribery policy to business associates who pose more than a low risk of bribery;

c) the policies, procedures and controls of the anti-bribery management system;

d) bribery risk assessment results (see 4.5);

e) anti-bribery training provided (see 7.3);

f) due diligence carried out (see 8.2);

g) the measures taken to implement the anti-bribery management system;

h) approvals and records of gifts, hospitality, donations and similar benefits given and received (see 8.7);

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;

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

A.18 Investigating and dealing with bribery

A.18.1 This document requires the organization to implement appropriate procedures on how to investigate and deal with any issue of bribery, or violation 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 violation 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 violation of anti-bribery controls. If the reports go in the first instance to another person, the organization's procedures should require 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 violation.

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 When any issue is identified, top management or the compliance function (as appropriate) should 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 start 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);

e) potential criminal, civil and administrative liability, financial loss and reputational damage for the organization and individuals;

f) any legal obligation, or benefit to the organization, to report to the authorities;

g) keeping the issue and investigation confidential until the facts have been established;

h) the need for top management to require the full co-operation of personnel in the investigation.

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

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

a) terminating, withdrawing from, or modifying the organization's involvement in, a project, transaction or contract;

b) repaying or reclaiming any improper benefit obtained;

c) disciplining responsible personnel (which, depending on the severity of the issue, could range from a warning for a minor offence to dismissal for a serious offence);

d) reporting the matter to the authorities;

e) if bribery has occurred, taking action to avoid or deal with any possible consequent legal offences (e.g. false accounting which may occur where a bribe is falsely described in the accounts, a tax offence where a bribe is wrongly deducted from income, or money-laundering where the proceeds of a crime are dealt with).

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

A.19 Monitoring

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

a) effectiveness of training;

b) effectiveness of controls, for example by sample testing outputs;

c) effectiveness of allocation of responsibilities for meeting anti-bribery management system requirements;

d) effectiveness in addressing compliance failures previously identified;

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

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

— non-compliance and "near misses" (an incident without adverse effect);

— instances where anti-bribery requirements are not met;

— instances where objectives are not achieved;

— the status of culture of compliance.

NOTE. See ISO 19600.

The organization can periodically perform self-assessments, either in the whole organization, or in parts of it, to assess the effectiveness of the anti-bribery management system (see 9.4).

A.20 Planning and implementing changes to the anti-bribery management system

A.20.1 The adequacy and effectiveness of the anti-bribery management system should be assessed on a continual and regular basis through several methods, e.g. reviews by internal audits (see 9.2), management (see 9.3) and the anti-bribery compliance function (see 9.4).

A.20.2 The organization should consider the results and outputs of such assessments to determine if there is a need or opportunity to change the anti-bribery management system.

A.20.3 In order to help ensure that the integrity of the anti-bribery management system and its effectiveness is retained, changes in individual elements of the management system should take into account the dependency and the impact of such change on the effectiveness of the management system as a whole.

A.20.4 When the organization determines the need for changes to the anti-bribery management system, such changes should be carried out in a planned manner by considering the following:

a) the purpose of the changes and their potential consequences;

b) the integrity of the anti-bribery management system;

c) the availability of resources;

d) the allocation or reallocation of responsibilities and authority;

e) the rate, extent and timeframe of implementing the changes.

A.20.5 Enhancements of the anti-bribery management system as a result of measures taken in reaction to any nonconformity (see 10.1) and resulting from continual improvements (see 10.2) should be carried out under the same approach as stated under A.20.4 above.

A.21 Public officials

The term "public official" (see 3.27) is defined broadly in many anti-corruption laws.

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

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, e.g. the World Bank, the United Nations, the International Monetary Fund;

f) employees of state-owned enterprises, unless the enterprise operates on a normal commercial basis in the relevant market, i.e. on a basis which is substantially equivalent to that of a private enterprise, without preferential subsidies or other privileges (see Reference [17]).

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

A.22 Anti-bribery initiatives

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

Bibliography

[1] ISO 9000, *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/IEC 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/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[10] ISO 31000, *Risk management — Principles and guidelines*

[11] ISO Guide 73, *Risk management — Vocabulary*

[12] ISO/IEC Guide 2, *Standardization and related activities — General vocabulary*

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

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

[15] Organization for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents, Paris, 2010

[16] Organization for Economic Co-operation and Development, Good Practice Guidance on Internal Controls, Ethics, and Compliance, Paris, 2010

[17] Organization for Economic Co-operation and Development, Commentaries on the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 21 November 1997

[18] United Nations Global Compact/Transparency International, Reporting guidance on the 10th principle against corruption, 2009

[19] 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

Bibliography (*continued*)

[20] International Chamber of Commerce, Rules on Combating Corruption, Paris, 2011

[21] Transparency International, Business Principles for Countering Bribery and associated tools, Berlin, 2013

[22] Transparency International, Corruption Perceptions Index

[23] Transparency International, Bribe Payers Index

[24] World Bank, Worldwide Governance Indicators

[25] International Corporate Governance Network, ICGN Statement and Guidance on Anti-Corruption Practices, London, 2009

[26] World Economic Forum, Partnering Against Corruption Principles for Countering Bribery, An Initiative of the World Economic Forum in Partnership with Transparency International and the Basel Institute on Governance, Geneva

[27] Committee of the Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework, May 2013

Acknowledgements

Members of Technical Committee on Anti-bibery management system

Dato' Shamshun Baharin	Malaysian Anti-corruption Commission
Mohd Jamil (Chairman)	
Ms Nur Asyikin Aminuddin/	Malaysian Association of Standards Users
Ms Saral James Maniam (Secretary)	
Mr Mohd Yunos Yusop	Association of Certified Fraud Examiners
Ms Haslina Halim/ Ir M. Ramuseren	Construction Industry Development Board
Mr Shahrul Mohd Tahir	Department of Standards Malaysia
Dr Zulkefli Ibrahim	Malaysian Administrative Modernisation and Management Planning Unit
Dato' Junipah Wandi	Malaysian Anti-corruption Commission
Ms Lauren Tam Kam Peng/	Malaysian Institute of Corporate Governance
Ms Nurul Afiqah Mohamad Rafi	
Dr Loi Kheng Min	Malaysian International Chamber of Commerce and Industry
Mr Oliver Wee Hiang Chyn	Master Builders Association Malaysia
Mr Alan Kirupakaran	Prime Minister's Department
Ms Lucy Wong Kam Yang	The Institute of Internal Auditors Malaysia
Dr Mohd Nizam Mohd Ali	The Malaysian Institute of Integrity