



**International
Standard**

ISO 37001

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

*Systemes de management anti-corruption — Exigences et
recommandations de mise en œuvre*

**Second edition
2025-02**



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved.

ISO publications, in their entirety or in fragments, are owned by ISO. They are licensed, not sold, and are subject to the terms and conditions set forth in the ISO End Customer License Agreement, the License Agreement of the relevant ISO member body, or those of authorized third-party distributors.

Unless otherwise specified or required for its implementation, no part of this ISO publication may be reproduced, distributed, modified, or used in any form or by any means, electronic or mechanical, including photocopying, scanning, recording, or posting on any intranet, internet, or other digital platforms, without the prior written permission of ISO, the relevant ISO member body or an authorized third-party distributor.

This publication shall not be disclosed to third parties, and its use is strictly limited to the license type and purpose specified in the applicable license grant. Unauthorized reproduction, distribution, or use beyond the granted license is prohibited and may result in legal action.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	v
Introduction	viii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	6
4.1 Understanding the organization and its context.....	6
4.2 Understanding the needs and expectations of interested parties.....	6
4.3 Determining the scope of the anti-bribery management system.....	7
4.4 Anti-bribery management system.....	7
4.5 Bribery risk assessment.....	7
5 Leadership	8
5.1 Leadership and commitment.....	8
5.1.1 Governing body.....	8
5.1.2 Top management.....	8
5.1.3 Anti-bribery culture.....	9
5.2 Anti-bribery policy.....	9
5.3 Roles, responsibilities and authorities.....	10
5.3.1 General.....	10
5.3.2 Anti-bribery function.....	10
5.3.3 Delegated decision-making.....	10
6 Planning	11
6.1 Actions to address risks and opportunities.....	11
6.2 Anti-bribery objectives and planning to achieve them.....	11
6.3 Planning of changes.....	12
7 Support	12
7.1 Resources.....	12
7.2 Competence.....	12
7.2.1 General.....	12
7.2.2 Employment process.....	12
7.3 Awareness.....	13
7.3.1 Awareness of personnel.....	13
7.3.2 Training for personnel.....	13
7.3.3 Training for business associates.....	14
7.3.4 Awareness and training programmes.....	14
7.4 Communication.....	14
7.5 Documented information.....	15
7.5.1 General.....	15
7.5.2 Creating and updating documented information.....	15
7.5.3 Control of documented information.....	15
8 Operation	16
8.1 Operational planning and control.....	16
8.2 Due diligence.....	16
8.3 Financial controls.....	16
8.4 Non-financial controls.....	16
8.5 Implementation of anti-bribery controls by controlled organizations and by business associates.....	17
8.6 Anti-bribery commitments.....	17
8.7 Gifts, hospitality, donations and similar benefits.....	18
8.8 Managing inadequacy of anti-bribery controls.....	18
8.9 Raising concerns.....	18
8.10 Investigating and dealing with bribery.....	18

ISO 37001:2025(en)

9	Performance evaluation	19
9.1	Monitoring, measurement, analysis and evaluation.....	19
9.2	Internal audit	19
9.2.1	General	19
9.2.2	Internal audit programme	20
9.2.3	Audit procedures, controls and systems.....	20
9.2.4	Objectivity and impartiality	20
9.3	Management review	20
9.3.1	General	20
9.3.2	Management review inputs	21
9.3.3	Management review results.....	21
9.4	Review by anti-bribery function	21
10	Improvement	22
10.1	Continual improvement.....	22
10.2	Nonconformity and corrective action.....	22
Annex A (informative) Guidance on the use of this document		23
Bibliography		46

Foreword

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

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

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

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

This document was prepared by Technical Committee ISO/TC 309, *Governance of organizations*.

This second edition cancels and replaces the first edition (ISO 37001:2016), which has been technically revised. It also incorporates the Amendment ISO 37001:2016/Amd 1:2024.

The main changes are as follows:

- subclauses were added on climate change and stressing the importance of the compliance culture;
- conflicts of interest were addressed;
- the concept of the anti-bribery function was clarified;
- the wording was harmonized with other standards where appropriate and reasonable;
- the latest harmonized structure was introduced.

Licensing and use terms

The ISO publications, as well as any updates and/or corrections, and any intellectual property or other rights pertaining thereto, are owned by ISO. ISO publications are licensed, not sold. Nothing in this document shall operate to assign or transfer any intellectual property rights from ISO to the user. The ISO publications are protected by copyright law, database law, trademark law, unfair competition law, trade secrecy law, or any other applicable law, as the case may be. Users acknowledge and agree to respect ISO's intellectual property rights in the ISO publications.

The use of ISO publications is subject to the terms and conditions of the applicable licensing agreement.

ISO publications are provided under different licensing agreement types ("License Type") allowing a non-exclusive, non-transferable, limited, revocable right to use/access the ISO publications for one or more of the following purposes described below ("Purpose"), which may be internal or external in scope. The applicable Purpose(s) must be captured in the licensing agreement.

ISO 37001:2025(en)

a) License Type:

- i. a single registered end-user license (watermarked in the user's name) for the specified Purpose. Under this license the user cannot share the ISO Publication with anyone, including on a network;
- ii. a network license for the specified Purpose. The network license may be assigned to either unnamed concurrent end-users or named concurrent end-users within the same organization.

b) Purpose:

- i. **Internal Purpose:** internal use only within user's organization, including but not limited to own implementation ("Internal Purpose").

The scope of permitted internal use is specified at the time of purchase or through subsequent agreement with ISO, the ISO member body in the user's country, any other ISO member body or an authorized third-party distributor, including any applicable internal reproduction rights (such as internal meetings, internal training programs, preparation of certification services, integration or illustration in internal manuals, internal training materials, and internal guidance documents). Each internal use must be explicitly specified in the purchase order, and specific fees and requirements will apply to each permitted use.

- ii. **External Purpose:** external use, including but not limited to certification services, consulting, training, digital services by user/user's organization to third parties, as well as for commercial and non-commercial purposes ("External Purpose").

The scope of permitted external use is specified at the time of purchase or through subsequent agreement with ISO, the ISO member body in user's country, any other ISO member body or an authorized third-party distributor, including any applicable external reproduction rights (e.g. in publications, products, or services marketed and sold by user/user's organization). Each external use must be explicitly specified in the purchase order, and specific fees and requirements will apply to each permitted use.

Unless users have been granted reproduction rights according to the above provisions, they are not granted the right to share or sub-license the ISO publications in- or outside their organization for either Purpose. If users wish to obtain additional reproduction rights for ISO publications or their content, users may contact ISO or the ISO member body in their country to explore their options.

In case the user or the user's organization is granted a license for the External Purpose of providing any or all activities in the delivery of certification services, or for auditing for a customer, the user or user's organization agrees to verify that the organization operating under the management system subject to certification or auditing has obtained a license for its own implementation of the ISO Standard used for the certification or auditing from the ISO member body in their country, any other ISO member body, ISO or an authorized third-party distributor. This verification obligation shall be included in the applicable license agreement obtained by the user or user's organization.

The ISO publications shall not be disclosed to third parties, and Users shall use them solely for the purpose specified in the purchase order and/or applicable licensing agreement. Unauthorized disclosure or use of ISO publications beyond the licensed purpose is prohibited and may result in legal action.

Use restrictions

Except as provided for in the applicable License Agreement and subject to a separate license by ISO, the ISO member body in user's country, any other ISO member body or an authorized third-party distributor, users are not granted the right to:

- use the ISO Publications for any purpose other than the Purpose;
- grant use or access rights to the ISO Publications beyond the License Type;
- disclose the ISO Publications beyond the intended Purpose and/or License Type;

ISO 37001:2025(en)

- sell, lend, lease, reproduce, distribute, import/export or otherwise commercially exploit ISO Publication(s). In the case of joint standards (such as ISO/IEC standards), this clause shall apply to the respective joint copyright ownership;
- assign or otherwise transfer ownership of the ISO Publications, in whole or in fragments, to any third party.

Regardless of the License Type or Purpose for which users are granted access and use rights for ISO publications, users are not permitted to access or use any ISO publications, in whole or in fragments, for any machine learning and/or artificial intelligence and/or similar purposes, including but not limited to accessing or using them (i) as training data for large language or similar models, or (ii) for prompting or otherwise enabling artificial intelligence or similar tools to generate responses. Such use is only permitted if expressly authorized through a specific license agreement by the ISO member body in the requester's country, another ISO member body, or ISO. Requests for such authorization may be considered on a case-by-case basis to ensure compliance with intellectual property rights.

If ISO, or the ISO member body in the user's country, has reasonable doubt that users are not compliant with these terms, it may request in writing to perform an audit, or have an audit performed by a third-party auditor, during business hours at user's premises or via remote access.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

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^[19] and the United Nations Convention against Corruption^[18] 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 help 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.

This document can be used in conjunction with other management system standards (e.g. ISO 9001, ISO 14001, ISO/IEC 27001, ISO 37301 and ISO 37002) and management standards (e.g. ISO 26000 and ISO 31000).

Guidance for the governance of organizations is specified in ISO 37000 and requirements for a general compliance management system are specified in ISO 37301.

Anti-bribery management systems — Requirements with guidance for use

1 Scope

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

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

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

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

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

NOTE 2 The measures necessary to prevent, detect and mitigate the risk of bribery by the organization can be different from the measures used to prevent, detect and respond to bribery of the organization (or its personnel or business associates acting on the organization's behalf). See [A.8](#) for guidance.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

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

**3.1
bribery**

offering, promising, giving, accepting or soliciting of an undue advantage of any value (which can 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)

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

Note 2 to entry: If the organization is part of a larger entity, the term “organization” refers only to the part of the larger entity that is within the scope of the anti-bribery *management system* (3.5).

**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: An interested party can be internal or external to the organization.

**3.4
requirement**

need that is stated and obligatory

Note 1 to entry: 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.

Note 2 to entry: “Generally implied” means that it is custom or common practice for the *organization* (3.2) and *interested parties* (3.3) that the need or expectation under consideration is implied.

Note 3 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.14).

**3.5
management system**

set of interrelated or interacting elements of an *organization* (3.2) to establish *policies* (3.10) and *objectives* (3.11), as well as *processes* (3.15) to achieve those objectives

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

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

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

**3.6
top management**

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

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

ISO 37001:2025(en)

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

Note 3 to entry: Organizations can be organized depending on which legal framework they are obliged to operate under and also according to their size, sector, etc. Some organizations have both a *governing body* (3.7) and *top management* (3.6), 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

person or group of people who have ultimate accountability for the whole *organization* (3.2)

Note 1 to entry: A governing body can be explicitly established in a number of formats including, but not limited to, a board of directors, supervisory board, sole director, joint and several directors, or trustees.

Note 2 to entry: ISO management system standards make reference to the term “top management” to describe a role that, depending on the standard and organizational context, reports to, and is held accountable by, the governing body.

Note 3 to entry: Not all organizations, particularly small and medium organizations, will have a governing body separate from top management. In such cases, top management exercises the role of the governing body.

[SOURCE: ISO 37000:2021, 3.3.4, modified — The Notes to entry were reordered: Note 2 to entry is now Note 1 to entry; Note 3 to entry is now Note 2 to entry; and Note 3 to entry was added.]

3.8 anti-bribery 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 are achieved

3.10 policy

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

3.11 objective

result to be achieved

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

Note 2 to entry: Objectives can relate to different disciplines (such as finance, sales and marketing, procurement, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product or *process* (3.15).

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

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

3.12 risk

effect of uncertainty on objectives

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

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

Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood 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

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

Note 2 to entry: Documented information can refer to:

- the *management system* (3.5), 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 that uses or transforms inputs to deliver a result

Note 1 to entry: Whether the result of a process is called an output, a product or a service depends on the context of the reference.

**3.16
performance**
measurable result

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

Note 2 to entry: Performance can relate to managing activities, *processes* (3.15), products, services, systems or *organizations* (3.2).

**3.17
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.

**3.18
measurement**
process (3.15) to determine a value

**3.19
audit**

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

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

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

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

**3.20
conformity**

fulfilment of a *requirement* (3.4)

3.21

nonconformity

non-fulfilment of a *requirement* (3.4)

3.22

corrective action

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

3.23

continual improvement

recurring activity to enhance *performance* (3.16)

3.24

personnel

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

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

Note 2 to entry: See [A.8](#) for guidance on temporary staff or workers.

3.25

business associate

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

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

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

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

3.26

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](#).

3.27

third party

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

Note 1 to entry: All *business associates* (3.25) are third parties, but not all third parties are business associates.

3.28

conflict of interest

situation in which an interested party has personal interest or organizational interest, directly or indirectly, that can compromise, or interfere with, the ability to act impartially in carrying out their duties in the best interest of the organization

Note 1 to entry: There can be different types of personal interests: business, financial, family, professional, religious or political.

Note 2 to entry: Organizational interest relates to the interests of an organization or part of an organization (e.g. team or department) rather than an individual.

[SOURCE: ISO 37009:—¹], 3.14]

3.29

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* (3.25) and *personnel* (3.24)

3.30

anti-bribery culture

values, ethics, beliefs and conduct that exist throughout an *organization* (3.1) and interact with the organization's structures and control systems to produce behavioural norms that are conducive to the anti-bribery *policy* (3.10) and the anti-bribery *management system* (3.5)

Note 1 to entry: This term has been adapted from ISO 37301:2021, 3.28, "compliance culture".

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 intended result(s) of its anti-bribery management system. These issues 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.

The organization shall determine whether climate change is a relevant issue.

NOTE An organization has control over another organization if it directly or indirectly controls the management of the organization (see A.13).

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

- a) the interested parties that are relevant to the anti-bribery management system;
- b) the relevant requirements of these interested parties;
- c) which of these requirements will be addressed through the anti-bribery management system.

NOTE 1 Relevant interested parties can have requirements related to climate change.

NOTE 2 In identifying the requirements of interested parties, an organization can distinguish between mandatory requirements and the non-mandatory expectations of, and voluntary commitments to, interested parties.

1) Under preparation. Stage at the time of publication: ISO/DIS 37009:2025.

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, implement, maintain and continually 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 be documented and shall contain measures designed to identify and evaluate the risk of bribery, and to prevent, detect and respond to the risk of bribery.

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

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

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

4.5 Bribery risk assessment

4.5.1 The organization shall undertake bribery risk assessment(s) at planned intervals, which shall:

- a) identify the bribery risks the organization can 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) at planned intervals 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 continually 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 separate 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) receiving and reviewing, at planned intervals, 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, its intended results and its effectiveness.

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

For more guidance about governing body and top management roles see ISO 37000:2021, 4.2.3.

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 policy and anti-bribery objectives are established;
- b) ensuring the integration of the anti-bribery management system requirements into the organization's business processes;
- c) ensuring that the resources needed for the anti-bribery management system are available;
- d) communicating internally and externally regarding the anti-bribery policy;
- e) communicating 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 achieves its intended result(s);
- 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 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 to raise concerns about suspected and actual bribery (see [8.9](#));
- l) ensuring that no personnel will suffer retaliation, discrimination or disciplinary action (except where the individual participated in the violation) [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 of the anti-bribery management system, or for refusing to engage in bribery, even if such refusal can result in the organization losing business;

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

NOTE 1 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.

NOTE 2 See [Clause A.5](#) for guidance.

5.1.3 Anti-bribery culture

The organization shall develop, maintain and promote an anti-bribery culture at all levels within the organization.

The governing body, top management and management shall demonstrate an active, visible, consistent and sustained commitment towards a common standard of behaviour and conduct that is required throughout the organization.

Top management shall encourage behaviour that supports the anti-bribery policy and the anti-bribery management system. It shall prevent and not tolerate behaviour that compromises anti-bribery.

NOTE See [Clause A.5](#) for guidance.

5.2 Anti-bribery policy

Top management shall establish 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 anti-bribery objectives;
- e) includes a commitment to meet applicable 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 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 within the organization;
- be available to interested parties, as appropriate;
- be communicated to business associates who pose more than a low risk of bribery.

5.3 Roles, responsibilities and authorities

5.3.1 General

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

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

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

The governing body, top management and all other personnel shall be responsible for understanding, complying with and applying the anti-bribery management system, as it relates to their role in the organization.

5.3.2 Anti-bribery function

The anti-bribery function shall have the responsibility and authority for:

- a) ensuring that the anti-bribery management system conforms to the requirements of this document;
- b) reporting on the performance of the anti-bribery management system to the governing body and top management.
- c) overseeing the design and implementation by the organization of the anti-bribery management system;
- d) providing advice and guidance to personnel and interested parties on the anti-bribery management system and issues relating to bribery;

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

The anti-bribery function shall have direct and prompt access to the governing body 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.

NOTE See [Clause A.6](#) for guidance.

Top management can assign some or all of the anti-bribery function to parties 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.

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 at planned intervals 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 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](#), and the requirements referred to in [4.2](#) and determine the risks and opportunities that need to be addressed to:

- a) give assurance that the anti-bribery management system can achieve its intended result(s);
- b) prevent, or reduce, undesired effects;
- c) achieve continual improvement;
- d) monitor the effectiveness of the anti-bribery management system.

The organization shall plan:

- i) actions to address these risks and opportunities;
- ii) 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 objectives at relevant functions and levels.

The anti-bribery objectives shall:

- a) be consistent with the anti-bribery policy;
- b) be measurable (if practicable);
- c) take into account applicable requirements;
- d) be monitored;
- e) be communicated;
- f) be updated as appropriate.
- g) be available as documented information;
- h) be achievable.

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

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

6.3 Planning of changes

When the organization determines the need for changes to the anti-bribery management system, the changes shall be carried out in a planned manner.

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

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 the necessary competence, and evaluate the effectiveness of the actions taken.

Appropriate documented information shall be available as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring 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

ISO 37001:2025(en)

- 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).
- e) personnel are made aware of the necessity to report potential and actual conflicts of interest.

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

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 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;
- b) performance bonuses, performance targets and other incentivizing elements of remuneration are reviewed at planned intervals, to verify that there are reasonable safeguards in place to prevent them from encouraging bribery;
- c) such personnel, top management, and the governing body, file a declaration at planned intervals proportionate with the identified bribery risk, confirming their compliance with the anti-bribery policy and the anti-bribery management system.

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

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

7.3 Awareness

7.3.1 Awareness of personnel

Personnel shall be aware of:

- a) the anti-bribery policy, procedures and anti-bribery management system, and their duty to comply;
- b) their contribution to the effectiveness of the anti-bribery management system, including the benefits of improved anti-bribery performance and of reporting suspected bribery;
- c) the implications of not conforming with the anti-bribery management system requirements;
- d) anti-bribery procedures and anti-bribery management system, and their duty to comply;
- e) the benefits of reporting suspected bribery;
- f) how and to whom they are able to report any concerns (see [8.9](#)).

The organization shall retain documented information on the awareness program, and when and to whom it was provided.

7.3.2 Training for personnel

The organization shall provide adequate and appropriate anti-bribery 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) applicable policies and procedures;
- 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) information on available training and resources.

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

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of personnel or business associates or the hiring or contracting of the same.

7.3.3 Training for business associates

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

For the business associates for which such training is necessary, the organization shall retain documented information on the training procedures, the content of the training, and when and to whom it was provided.

NOTE The 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.

7.3.4 Awareness and training programmes

Personnel shall be provided with anti-bribery awareness and training from the time of commencement of employment and 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 updated at planned intervals, as necessary, to reflect relevant new information.

NOTE 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 in appropriate languages 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.

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

- the size of organization and its type of activities, processes, products and services;
- the complexity of processes and their interactions;
- the competence of personnel.

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

NOTE 3 See [Clause A.17](#) for guidance.

7.5.2 Creating and updating documented information

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 and control the processes needed to meet requirements, and to implement the actions determined in [Clause 6](#), by:

- a) establishing criteria for the processes;
- b) implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

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 externally provided processes, products or services that are relevant to the anti-bribery management system are controlled.

These processes shall include the specific controls referred to in [8.2](#) to [8.10](#).

NOTE An external organization is outside the scope of the management system, although the externally provided function or process is within the scope.

8.2 Due diligence

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

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

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

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

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

NOTE 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, mergers and acquisitions and regulatory activities.

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

NOTE 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](#)).

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 can 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 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 can 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.

NOTE 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).

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

NOTE 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.

NOTE 4 For further guidance, see ISO 37002.

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 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.

NOTE 1 See [Clause A.18](#) for guidance.

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

NOTE 3 For further guidance, see ISO/TS 37008.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

- a) what needs to be monitored and measured;
- b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
- c) when the monitoring and measuring shall be performed;
- d) when the results from monitoring and measurement shall be analysed and evaluated.

Documented information shall be available as evidence of the results.

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

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

9.2 Internal audit

9.2.1 General

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

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

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

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

NOTE 3 See [Clause A.16](#) for guidance.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

- a) define the audit objectives, criteria and scope for each audit;
- b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
- c) ensure that the results of the audits are reported to relevant managers, the anti-bribery function, top management and, as appropriate, the governing body.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.2.3 Audit procedures, controls and systems

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;
- 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 Objectivity and impartiality

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 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 function is responsible; or
- c) appropriate personnel 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.

9.3 Management review

9.3.1 General

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

The governing body shall undertake reviews of the top management's implementation of the anti-bribery management system, at planned intervals, based on information provided by top management and the anti-bribery function and any other information that the governing body requests or obtains.

9.3.2 Management review inputs

The management review shall include:

- 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) changes in needs and expectations of interested parties that are relevant to the anti-bribery management system;
- d) 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;
- e) opportunities for continual improvement ;
- f) effectiveness of actions taken to address bribery risks.

9.3.3 Management review results

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

Documented information shall be available as evidence of the results of management reviews.

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

9.4 Review by anti-bribery function

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

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

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

NOTE 1 The frequency of such reports depends on the organization's structure and needs.

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

10 Improvement

10.1 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.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

- a) react 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 can 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.

Documented information shall be available as evidence of:

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

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

Annex A (informative)

Guidance on the use of this document

A.1 General

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

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

A.2 Scope of the anti-bribery management system

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

The organization can choose to implement this anti-bribery management system as a separate system, or as an integrated part of an overall compliance management system (in which case the organization can refer for guidance to ISO 37301). 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 can 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 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 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 Anti-bribery management system

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 and top management of an organization:

- 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.

A.3.2 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.3.3 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.3.4 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 needs 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.3.5 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 can 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.

A.4.2 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 can 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.

ISO 37001:2025(en)

- 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 can 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 can 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.

A.4.3 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.4.4 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.4.5 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.4.6 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 reviewed at planned intervals 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 and ISO 31022.

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

A.5.1 General

A.5.1.1 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 receive information at planned intervals regarding the performance of the management system through the management review process (this can be to the entire governing body, or to a committee of the body, such as the audit committee). In this respect, the anti-bribery function should be able to report information about the management system directly to the governing body (or the appropriate committee thereof).

A.5.1.2 It is possible that some organizations, particularly smaller ones, do not have a separate governing body, or that the roles of the governing body and executive management are 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.5.2 Anti-bribery culture

A.5.2.1 Factors that support the development of an anti-bribery culture include:

- management actively implementing, promoting and visibly abiding by the organization's anti-bribery culture;
- mentoring and leading by example on the importance of the organization's anti-bribery culture;
- an emphasis on the organization's anti-bribery culture in the induction programme for personnel;
- on-going communication with personnel on the organization's anti-bribery culture;
- visible recognition of achievements of personnel in promoting the organization's anti-bribery culture;
- consistency in the treatment of behaviour by personnel that compromises the organization's anti-bribery culture, regardless of position.

A.5.2.2 Evidence of an anti-bribery culture is indicated by the degree to which:

- the items above are documented, implemented and practiced;
- personnel believe that the items above have been implemented;
- personnel understand the relevance of the organization's anti-bribery culture to their position, their own activities and to those of their business unit;
- the role and objectives of the anti-bribery management system, notably of the anti-bribery policy, of related procedures, and of the anti-bribery function, are valued by personnel;
- corrective actions to address behaviour by personnel that compromises the organization's anti-bribery management system are 'owned' and actioned, as required, at all appropriate levels of the organization.

A.6 Anti-bribery function

A.6.1 The number of people working in the anti-bribery 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 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 workload justifies it, the anti-bribery 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 function, and this is acceptable provided that an appropriate manager within the organization retains overall responsibility for and authority over the anti-bribery function and supervises the services provided by the third party.

A.6.2 This document requires that the anti-bribery 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 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 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 function has direct access to top management and to the governing body, in order to communicate relevant information. The function should not have to report solely to another manager in the chain who then reports to top management, as this increases the risk that the message given by the anti-bribery function is not fully or clearly received by top management. The anti-bribery function should also have a direct communications relationship to the governing body, 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 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 37301.

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 function.
- b) Physical resources: There should be the necessary physical resources in the organization, including in the anti-bribery 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 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

A.8.2.1 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 can 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 can occur if too much pressure is put on a manager to perform (e.g. if the manager can 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.

A.8.2.2 Personnel evaluations, promotions, bonuses and other rewards can 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.

A.8.2.3 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

A.8.3.1 The organization should identify, analyse and evaluate the risks of internal and external conflicts of interest. The organization should clearly inform all personnel of their duty to report any potential and actual 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,
- b) when a manager in a procurement function holds a financial interest in a supplier,
- c) when an organization's line manager has a personal financial interest in a competitor's business,
- d) when a director of an organization (who may have a non-executive role) or a member of top management has either legitimate or concealed personal interests or a position in a competing or a potentially acquiring organization.

A.8.3.2 The organization should keep a record of all declarations of conflict of interest, and of any circumstances of actual or potential conflicts of interest and of whether and what actions were taken to mitigate the conflict.

A.8.3.3 These should be reviewed at least once a year to ensure that they are still relevant and up to date.

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 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 the paragraphs on due diligence and conflict of interests above, the risk of inbound bribery can 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 can exploit existing control weaknesses for personal gain. Example procedures 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 are 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 can 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, 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 function does not have sufficient related experience, the organization should provide any training necessary for him or her to perform the anti-bribery 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 can 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 requirements to business associates identified under the requirements of [7.3.4](#) 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 can 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 [7.3.4](#) 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 can lead to bribery (this includes 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 can pay a bribe to a manager of the organization's customer to help the organization win the contract, and so can 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 can 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 can be because the organization would not have sufficient influence over the client or customer to be able to do so (e.g. 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](#).

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. Well-designed anti-bribery financial controls act as checks and balances to deter improper behaviour by raising the risk of detection and capturing information to enable investigation. Depending on the size of the organization and transaction, the financial controls implemented by an organization which can reduce the bribery risk can 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 management review at planned intervals of significant financial transactions;
- i) implementing independent financial audits at planned intervals and changing, also at planned intervals, 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 can 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 can 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;

ISO 37001:2025(en)

- 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 37301.

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 The 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 can 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 can 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 can be implemented by the business associate would not help mitigate the relevant risk (there would be no point in insisting that the business associate implements controls which would not help; however, in this case, the organization would be expected to take account of this factor in its risk assessment in order to inform the decision regarding how and whether to proceed with the relationship).

A.13.3.2 This reflects the reasonableness and proportionality of this document.

A.13.3.3 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.
- 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 to do so, the organization requires the business associate to implement anti-bribery controls in relation to the relevant transaction, project or activity.
 - 2) Where it is not practicable 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.13.3.4 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.

ISO 37001:2025(en)

- 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.13.3.5 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 may 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 (e.g. an agent or a minor supplier), the organization may require training for relevant employees, and controls over key payments and gifts and hospitality.

A.13.3.6 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).

A.13.3.7 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.13.3.8 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.13.3.9 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.13.3.10 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 can 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).

A.14.3 In these cases, the organization would not be required to obtain anti-bribery commitments from these low bribery risk suppliers or customers.

A.14.4 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.14.5 These commitments should as far as possible be obtained in writing. This can 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 can reasonably be perceived by a third party to be for the purpose of bribery.

A.15.2 The benefits referred to in [8.7](#) can 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;

ISO 37001:2025(en)

- 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 can, 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;
 - 2) permitting gifts and hospitality, but limiting them by reference to such factors as:
 - i) a maximum expenditure (which can 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 can, for example, be designed to:

- a) prohibit payments which are intended to influence, or can 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. 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 can, 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 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 programme or may engage a third party to implement certain portions of an existing programme.

A.16.2 The frequency of audit depends 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 can 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 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 can 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 anti-bribery 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 anti-bribery function as soon as possible. In some cases, the anti-bribery 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 anti-bribery 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 anti-bribery function, with a summary report of all minor issues being made to top management at planned intervals;
 - 2) major issues are reported straight away by the anti-bribery function to top management for top management decision on how to respond.

A.18.4 When any issue is identified, top management or the anti-bribery 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 can be the anti-bribery 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 can be necessary);
- 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 anti-bribery function as appropriate. If the results are reported to top management, they should also be communicated to the anti-bribery 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 can 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, can 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

A.19.1 Monitoring of the anti-bribery management system may include, for example, the following areas:

- a) effectiveness of training;
- b) effectiveness of controls, e.g. 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.

A.19.2 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 37301.

A.19.3 The organization can perform, at planned intervals, 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

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 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 [10.2](#)) and resulting from continual improvements (see [10.1](#)) should be carried out under the same approach.

A.21 Public officials

A.21.1 The term “public official” (see [3.26](#)) is defined broadly in many anti-corruption laws.

A.21.2 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.

A.21.3 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 [\[19\]](#)).

A.21.4 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 can 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 14001, *Environmental management systems — Requirements with guidance for use*
- [4] ISO/IEC 17000, *Conformity assessment — Vocabulary and general principles*
- [5] ISO 19011, *Guidelines for auditing management systems*
- [6] ISO 22000, *Food safety management systems — Requirements for any organization in the food chain*
- [7] ISO 26000, *Guidance on social responsibility*
- [8] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*
- [9] ISO 31000, *Risk management — Guidelines*
- [10] ISO 31022, *Risk management — Guidelines for the management of legal risk*
- [11] ISO 37000:2021, *Governance of organizations — Guidance*
- [12] ISO 37002, *Whistleblowing management systems — Guidelines*
- [13] ISO/TS 37008, *Internal investigations of organizations — Guidance*
- [14] ISO 37009:—, *Conflict of interest in organizations — Guidelines*
- [15] ISO 37301, *Compliance management systems — Requirements with guidance for use*
- [16] ISO/IEC Guide 2, *Standardization and related activities — General vocabulary*
- [17] United Nations Convention against Corruption, New York, 2004. Available at: https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf
- [18] Organization for Economic Co-operation and Development, *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents*, Paris, 2010
- [19] Organization for Economic Co-operation and Development, *Good Practice Guidance on Internal Controls, Ethics, and Compliance*, Paris, 2010
- [20] 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
- [21] United Nations Global Compact/Transparency International, *Reporting guidance on the 10th principle against corruption*, 2009
- [22] 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
- [23] International Chamber of Commerce, *Rules on Combating Corruption*, Paris, 2011
- [24] Transparency International, *Business Principles for Countering Bribery and associated tools*, Berlin, 2013
- [25] Transparency International, *Corruption Perceptions Index*
- [26] Transparency International, *Bribe Payers Index*

ISO 37001:2025(en)

- [27] World Bank, Worldwide Governance Indicators
- [28] International Corporate Governance Network, ICGN Statement and Guidance on Anti-Corruption Practices, London, 2009
- [29] 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
- [30] Committee of the Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework, May 2013



**ICS 03.100.02; 03.100.01;
03.100.70**

Price based on 47 pages

© ISO 2025
All rights reserved

iso.org

国际标准

ISO
37001

第1版
2025-02

反贿赂管理体系—要求及使用指南

Anti-bribery management systems—

Requirements with guidance for use

(雷泽佳翻译, 2025年3月)



ISO 37001-2025

©ISO 2025

本标准由雷泽佳翻译, 13087319462, leizejia@126.com

目 次

前言	III
引言	VI
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 组织的环境	7
4.1 理解组织及其环境	7
4.2 理解相关方的需求和期望	7
4.3 确定反贿赂管理体系的范围	8
4.4 反贿赂管理体系	8
4.5 贿赂风险评估	8
5 领导作用	8
5.1 领导作用和承诺	9
5.1.1 治理机构	9
5.1.2 最高管理者	9
5.1.3 反贿赂文化	10
5.2 反贿赂方针	10
5.3 岗位、职责和权限	10
5.3.1 总则	10
5.3.2 反贿赂职能	11
5.3.3 委托决策	11
6 策划	11
6.1 应对风险和机遇的措施	11
6.2 反贿赂目标及实现目标的策划	12
6.3 变更的策划	12
7 支持	12
7.1 资源	12
7.2 能力	13
7.2.1 总则	13
7.2.2 聘用过程	13
7.3 意识	14
7.3.1 人员的意识	14
7.3.2 人员的培训	14
7.3.3 商业伙伴的培训	14
7.3.4 意识和培训计划	15
7.4 反贿赂沟通	15
7.5 成文信息	15
7.5.1 总则	15
7.5.2 成文信息创建和更新	16
7.5.3 成文信息的控制	16
8 运行	16
8.1 运行的策划和控制	16
8.2 尽职调查	16
8.3 财务控制	17
8.4 非财务控制	17
8.5 受控组织和商业伙伴实施反贿赂控制	17
8.6 反贿赂承诺	18
8.7 礼品、招待、捐赠及类似利益	18

8.8 管理反贿赂控制的不足	18
8.9 提出疑虑	18
8.10 调查和处理贿赂	19
9 绩效评价	19
9.1 监视、测量、分析和评价	19
9.2 内部审核	20
9.2.1 总则	20
9.2.2 内部审核方案	20
9.2.3 审核程序、控制和系统	20
9.2.4 客观性和公正性	21
9.3 管理评审	21
9.3.1 总则	21
9.3.2 管理评审输入	21
9.3.3 管理评审结果	21
9.4 反贿赂职能部门的评审	22
10 改进	22
10.1 持续改进	22
10.2 不合格和纠正措施	22
附录 A (资料性) 本标准使用指南	24
参考文献	47

前 言

国际标准化组织（ISO）是由各国标准化团体（ISO 成员团体）组成的世界性的联合会。制定国际标准工作通常由 ISO 的技术委员会完成。各成员团体若对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与 ISO 保持联系的国际组织（官方的或非官方的）也可参加有关工作。ISO 与国际电工委员会（IEC）在电工技术标准方面保持密切合作的关系。

制定本标准及其后续标准维护的程序在 ISO/IEC 指引第 1 部分均有描述。应特别注意用于各不同类别 ISO 文件批准准则。本标准根据 ISO/IEC 导则第 2 部分的规则起草（见 www.iso.org/directives）。

本标准中的某些内容有可能涉及一些专利权问题，对此应引起注意。ISO 不负责识别任何这样的专利权问题。在标准制定期间识别的专利权细节将出现在引言/或收到的 ISO 专利权声明清单中（www.iso.org/patents）。

本标准中使用的任何商品名称仅为方便用户而提供的信息，并不构成认可。

ISO 与合格评定相关的特定术语和表述含义的解释以及 ISO 遵循的世界贸易组织（WTO）贸易技术壁垒（TBT）原则相关信息访问 www.iso.org/iso/foreword.html。

本标准由 ISO/TC 309（组织治理）技术委员会编制。

本第二版取消并代替第一版（ISO 37001:2016），该版已经过技术修订。本版还纳入了修正案 ISO 37001:2016/Amd 1:2024。

主要变更如下：

- 增加了关于气候变化和强调合规文化重要性的子条款；
- 解决了利益冲突问题；
- 澄清了反贿赂职能的概念；
- 在适当和合理的情况下，与其他标准的措辞保持一致；
- 引入了最新的协调结构。

许可和使用条款

ISO 出版物的使用需遵守适用许可协议的条款和条件。ISO 出版物根据不同的许可协议类型（“许可类型”）提供，允许非独占、不可转让、有限、可撤销的权利，以使用/访问 ISO 出版物，用于以下一个或多个目的（“目的”），这些目的可能是内部或外部范围的。适用的目的必须在许可协议中明确。

a) 许可类型：

1) 单一注册最终用户许可：

- 该许可为指定目的提供，并在用户姓名上加水印。
- 在此许可下，用户不能与任何人共享 ISO 出版物，包括在网络上共享。

2) 网络许可：

该许可为指定目的提供，可分配给同一组织内的未命名并发最终用户或命名并发最终用户。

b) 目的。

1) 内部目的:

——仅限于用户组织内部使用，包括但不限于自身实施。

允许的内部使用范围在购买时或通过 ISO、用户所在国家的 ISO 成员机构、任何其他 ISO 成员机构或授权第三方分销商达成的后续协议中指定。这包括任何适用的内部复制权利（如内部会议、内部培训计划、认证服务的准备、整合或说明在内部手册、内部培训材料和内部指导文件中）。每次内部使用必须在采购订单中明确指定，并且每次允许的使用都将适用特定的费用和要求。

2) 外部目的:

外部使用，包括但不限于由用户/用户组织向第三方提供的认证服务、咨询、培训、数字服务等，以及用于商业和非商业目的。

允许外部使用的范围在购买时或通过随后与国际标准化组织（ISO）、用户所在国家的 ISO 成员机构、任何其他 ISO 成员机构或授权第三方分销商达成的协议中指定，包括任何适用的外部复制权（例如，在用户/用户组织营销和销售的出版物、产品或服务中）。每次外部使用必须在采购订单中明确指定，并且每次允许的使用都将适用特定的费用和要求。

除非用户已根据上述规定获得复制权，否则用户无权在其组织内外出于任何目的共享或转授权 ISO 出版物。如果用户希望为 ISO 出版物或其内容获得额外的复制权，用户可以联系 ISO 或其所在国家的 ISO 成员机构以探讨其选择。

在用户或用户组织被授予提供认证服务交付中的任何或全部活动，或为客户进行审核的外部使用许可的情况下，用户或用户组织同意核实，受认证或审核的管理体系运行的组织已从其所在国家的 ISO 成员机构、任何其他 ISO 成员机构、ISO 或授权第三方分销商处获得了用于认证或审核的 ISO 标准自行实施的许可。此核实义务应包含在用户或用户组织获得的适用许可协议中。

ISO 出版物不得披露给第三方，用户应仅将其用于采购订单和/或适用许可协议中指定的目的。未经授权超出许可目的披露或使用 ISO 出版物是禁止的，并可能导致法律行动。

ISO 出版物根据不同类型的许可协议（“许可类型”）提供，允许非独占、不可转让、有限、可撤销的权利，以使用/访问 ISO 出版物，用于以下一个或多个目的（“目的”），这些目的可能是内部或外部范围的。适用的目的必须在许可协议中明确。

使用限制

除适用许可协议中另有规定，并需获得国际标准化组织（ISO）、用户所在国家的 ISO 成员机构、任何其他 ISO 成员机构或授权第三方分销商另行授予的许可外，用户无权：

——将 ISO 出版物用于除许可目的以外的任何目的；

——授予超出许可类型的 ISO 出版物使用或访问权限；

——超出预定目的和/或许可类型披露 ISO 出版物；

——出售、出借、出租、复制、分发、进出口或以其他方式商业利用 ISO 出版物。对于联合标准（如 ISO/IEC 标准），本条款适用于相应的联合版权所有权；

——将 ISO 出版物（全部或部分）的所有权转让给任何第三方。

无论用户为 ISO 出版物获得访问和使用权限的许可类型或目的如何，用户均不得整体或部分地访问或使用任何 ISO 出版物用于机器学习、人工智能和/或类似目的，包括但不限于将其作为 (i) 大型语言模型或类似模型的训练数据，或 (ii) 用于提示或以其他方式使人工智能或类似工具生成响应。此类使用仅在通过请求者所在国家的 ISO 成员机构、另一个 ISO 成员机构或 ISO 的特定许可协议明确授权的情况下才被允许。对于此类授权的请求，将逐例考虑以确保遵守知识产权。

如果 ISO 或用户所在国家的 ISO 成员机构有合理怀疑认为用户未遵守这些条款，其可书面要求在用户场所或通过远程访问在工作时间内进行审核，或由第三方审核员进行审核。

有关本标准的任何反馈或问题，应提交给用户的国家标准机构。这些机构的完整列表可在 www.iso.org/members.html 上找到。

引 言

贿赂是一种普遍存在的现象，它引发了严重的社会、道德、经济和政治疑虑，破坏了良好治理，阻碍了发展，并扭曲了竞争。贿赂侵蚀了正义，损害了人权，是缓解贫困的障碍。它还增加了商业活动的成本，给商业交易带来了不确定性，提高了商品和服务的价格，降低了产品和服务的质量，这可能导致生命和财产的损失，破坏对机构的信任，并干扰市场的公平和高效运行。

政府已经通过国际协议（如《经济合作与发展组织关于在国际商业交易中打击贿赂外国公职人员的公约》^[10]和《联合国反腐败公约》^[18]）以及国家法律，在解决贿赂问题方面取得了进展。在大多数司法管辖区，个人从事贿赂行为是违法的，并且有一种日益增长的趋势是，使组织以及个人都对贿赂行为承担责任。

然而，仅靠法律并不足以解决这个问题。组织有责任积极主动地参与打击贿赂。这可以通过反贿赂管理体系来实现，本标准旨在提供这样的管理体系，并通过领导层的承诺来建立诚信、透明、开放和合规的文化。组织的文化性质对于反贿赂管理体系的成功或失败至关重要。

一个管理良好的组织应有一项合规政策，并由适当的管理体系支持，以协助其履行法律义务和对诚信的承诺。反贿赂方针是整体合规政策的一个组成部分。反贿赂方针及其支持的管理体系有助于组织避免或减轻涉及贿赂的成本、风险和损害，促进商业交易中的信任和信心，并提升其声誉。

本标准反映了国际良好实践，可在所有司法管辖区使用。它适用于所有部门的小型、中型和大型组织，包括公共部门、私营部门和非营利部门。组织面临的贿赂风险因多种因素而异，如组织的规模、组织运营的地点和部门，以及组织活动的性质、规模和复杂性。本标准规定了组织根据其所面临的贿赂风险，实施合理且相称的政策、程序和控制措施。附件A提供了实施本标准要求的指导。

符合本标准并不能保证组织没有发生或将来不会发生贿赂行为，因为完全消除贿赂风险是不可能的。然而，本标准可以帮助组织实施旨在预防、检测和应对贿赂的合理且相称的措施。

本标准可以与其他管理体系标准（如ISO 9001、ISO 14001、ISO/IEC 27001、ISO 37301和ISO 37002）和管理标准（如ISO 26000和ISO 31000）结合使用。

关于组织治理的指导在ISO 37000中进行了规定，而一般合规管理体系的要求在ISO 37301中进行了规定。

反贿赂管理体系——要求及使用指南

1 范围

本标准规定了建立、实施、保持、评审和改进反贿赂管理体系的要求，并提供了相关指导。该体系可以独立存在，也可以融入整体管理体系中。本标准涉及组织活动相关的以下方面：

- 公共部门、私营部门和非营利部门的贿赂；
- 组织的贿赂行为；
- 组织人员代表组织或为了组织利益而进行的贿赂；
- 组织商业伙伴代表组织或为了组织利益而进行的贿赂；
- 对组织的贿赂；
- 与组织活动相关的对组织人员的贿赂；
- 与组织活动相关的对组织商业伙伴的贿赂；
- 直接和间接贿赂（例如，通过第三方或由第三方提供或接受的贿赂）。

本标准仅适用于贿赂问题。它规定了要求，并为旨在帮助组织预防、检测和应对贿赂，以及遵守适用于其活动的反贿赂法律和自愿承诺的管理体系提供了指导。

本标准的要求是通用的，旨在适用于所有组织（或组织的一部分），无论其类型、规模和活动性质如何，也无论其属于公共部门、私营部门还是非营利部门。这些要求的适用程度取决于4.1、4.2和4.5中指定的因素。

注1：见 A.2 以获取指导。

注2：组织为防止、检测和减轻自身贿赂风险所需的措施，可能与用于防止、检测和应对对组织（或其人员或代表组织行事的商业伙伴）的贿赂的措施不同。见 A.8 以获取指导。

2 规范性引用文件

本标准中无规范性引用文件。

3 术语和定义

以下术语和定义适用于本标准。

ISO（国际标准化组织）和IEC（国际电工委员会）维护用于标准化的术语数据库，其访问地址如下：

- ISO 在线浏览平台：<https://www.iso.org/obp>
- IEC Electropedia：<https://www.electropedia.org/>

3.1

贿赂 bribery

提供、承诺、给予、接受或索取任何价值的不当利益（无论是财务的或非财务的），无论地点如何，直接或间接地违反适用法律，以此作为引诱或奖励，促使个人就其职责绩效（3.16）采取或不采取行动。

注1：上述为一般定义，“贿赂”一词的含义由适用于组织（3.2）的反贿赂法律和由组织设计的反贿赂管理体系（3.5）进行具体规定。

3.2

组织 organization

为实现其目标（3.11），具有自身职责、权限和相互关系的个人或一群人。

注1：组织的概念包括但不限于个体经营者、公司、集团、商行、企事业单位、行政机构、合伙企业、慈善机构或研究机构，或其部分或组合，无论是否具有法人资格，无论公立还是私立。

注2：如果组织是更大实体的一部分，则“组织”一词仅指处于反贿赂管理体系（3.5）范围内的该更大实体的一部分。

3.3

相关方（推荐术语）interested party

利益相关者（认可术语）stakeholder

能够影响、被影响或自认为受到某个决定或活动影响的个人或组织（3.2）。

注1：相关方可以是组织内部的或外部的。

3.4

要求 requirement

明确表述的、必须履行的需求。

注1：ISO 管理体系标准中“要求”的核心定义是“明确表述的、通常隐含的或必须履行的需求或期望”。在反贿赂管理的背景下，“通常隐含的要求”不适用。

注2：“通常隐含”意味着对于组织（3.2）和相关方（3.3）而言，所考虑的需求或期望是习惯或常见做法所隐含的。

注3：规定的要求是明确表述的，例如在成文信息（3.14）中。

3.5

管理体系 management system

组织（3.2）中用于建立方针（3.10）和目标（3.11），以及实现这些目标的过程（3.15）的一组相互关联或相互作用的要素。

注1：管理体系可以针对一个领域或多个领域。

注2：管理体系要素包括组织的结构、岗位和职责、策划和运行。

注3：管理体系的范围可以包括整个组织、组织的特定和已识别的职能、组织的特定和已识别的部分，或跨一组组织的一个或多个职能。

3.6

最高管理者 top management

在最高层指挥和控制组织（3.2）的一个人或一组人。

注1：注释 1：最高管理者在组织内有授权和提供资源的权力。

注2：若管理体系（3.5）的范围仅覆盖组织的一部分，则最高管理者是指那些指挥并控制组织该部分的人员。

注3：组织的形式取决于其运营所遵照的法律框架及其规模大小、所属行业等。有些组织可能同时设有治理机构（3.7）和最高管理者，而有些组织则没有将职责分属于多个机构。在适用第 5 章的要求时，应考虑到这些关于组织及其职责的不同情况。

3.7

治理机构 governing body

对组织（3.2）的整体活动、治理和政策承担最终责任并行使权力的个人或一组人，最高管理者（3.6）向其报告并对其负责。

注1：治理机构可以以多种形式明确设立，包括但不限于董事会、监事会、唯一董事、联合董事或受托人。

注2：ISO 管理体系标准使用“最高管理者”一词来描述一个岗位，该岗位根据标准和组织背景的不同，向治理机构报告并对其负责。

注3：并非所有组织，特别是小型和中型组织，都会有独立于最高管理者的治理机构。在这种情况下，最高管理者履行治理机构的职责。

[来源：ISO 37000:2021, 3.3.4, 已修改——注的排序已更改；原注2现为注1；原注3现为注2；并增加了注3。]

3.8

反贿赂职能 anti-bribery function

负责反贿赂管理体系（3.5）运行的个人或群体。

3.9

有效性 effectiveness

完成策划的活动并实现策划结果的程度。

3.10

方针 policy

由最高管理者（3.6）或治理机构（3.7）正式发布的组织（3.2）的宗旨和方向。

3.11

目标 objective

要实现的结果。

注1：目标可以是战略性的、战术性的或操作性的。

注2：目标可以与不同的领域相关（如财务、销售和市场营销、采购、健康和环境以及安全）。它们可以是组织范围内的，也可以是特定于项目、产品或过程（3.15）的。

注3：目标可以用其他方式表达，例如作为预期结果、目的、操作准则、反贿赂目标或使用具有相似含义的其他词语（如宗旨、目标或指标）。

注4：在反贿赂管理体系（3.5）的语境中，组织（3.2）根据反贿赂方针（3.10）设定反贿赂目标，以实现特定结果。

3.12

风险 risk

不确定性对目标的影响。

注1：影响是偏离预期的——无论是正面的还是负面的。

注2：不确定性是与事件、其后果或可能性相关的信息、理解或知识存在缺陷的状态，即使是部分缺陷。

注3：风险通常通过参考潜在事件和后果，或这两者的组合来描述其特征。

注4：风险通常用事件（包括环境变化）的后果及其相关发生可能性的组合来表达。

3.13

能力 competence

运用知识和技能实现预期结果的能力。

3.14

成文信息 documented information

组织（3.2）需要控制和保持的信息及其所承载的媒介。

注1：成文信息可以是任何格式和媒介，且可以来自任何来源。

注2：成文信息可以指：

—— 管理体系（3.5），包括相关过程（3.15）；

—— 为组织运营而创建的信息（文件）；

—— 实现结果的证据（记录）。

3.15

过程 process

相互关联或相互作用的一组活动，这些活动使用或转化输入以产生结果。

注1：注释 1：一个过程的结果是否被称为输出、产品或服务，取决于参考的语境。

3.16

绩效 performance

可测量的结果。

注1：绩效可以与定量或定性的发现相关。

注2：绩效可以与管理活动、过程（3.15）、产品、服务、体系或组织（3.2）相关。

3.17

监视 monitoring

确定体系、过程（3.15）或活动的状态。

注1：为了确定状态，可能需要检查、监督或批判性地观察。

3.18

测量 measurement

确定值的过程（3.15）。

3.19

审核 audit

一种系统而独立的过程（3.15），用于获取证据并客观地评价它，以确定审核准则被满足的程度。

注1：审核可以是内部审核（第一方）或外部审核（第二方或第三方），也可以是结合审核（结合两个或多个学科）。

注2：内部审核由组织（3.2）自身或代表其进行的外部方进行。

注3：“审核证据”和“审核准则”在 ISO 19011 中有定义。

3.20

符合性 conformity

满足要求（3.4）。

3.21

不符合性 nonconformity

未满足要求（3.4）。

3.22

纠正措施 corrective action

为消除不符合（3.21）的原因并防止其再次发生的措施。

3.23

持续改进 continual improvement

为增强绩效（3.16）而反复进行的活动。

3.24

人员 personnel

组织的 (3.2) 董事、官员、雇员、临时工作人员或工人，以及志愿者。

注1：不同类型的人员会带来不同类型和程度的贿赂风险 (3.12)，组织在贿赂风险评估和贿赂风险管理程序中可以对其采取不同的处理方式。

注2：关于临时工作人员或工人的指导，请见 A.8。

3.25

商业伙伴 business associate

与组织 (3.2) 已经建立或计划建立某种形式的商业关系的外部方。

注1：商业伙伴包括但不限于客户、客户、合资企业、合资伙伴、联合体伙伴、外包提供商、承包商、咨询师、分包商、供方、销售商、顾问、代理、分销商、代表、中介和投资者。此定义故意宽泛，应根据组织的贿赂风险 (3.12) 状况来解释，以适用于那些可能使组织合理暴露于贿赂风险的商业伙伴。

注2：不同类型的商业伙伴会带来不同类型和程度的贿赂风险，组织 (3.2) 对不同类型的商业伙伴的影响能力也会有所不同。组织的贿赂风险评估和贿赂风险管理程序可以对不同类型的商业伙伴采取不同的处理方式。

注3：本文中的“商业”一词可广义解释为与组织存在目的相关的活动。

3.26

公职人员 public official

通过任命、选举或继承而担任立法、行政或司法职务的人，或行使公共职能的任何人，包括为公共机构或公共企业行使职能的人，或任何国内或国际公共组织的官员或代理人，或任何公职候选人。

注1：关于可被视为公职人员的个人的示例，请见 A.21。

3.27

第三方 third party

独立于组织 (3.2) 的个人或机构。

注1：注：所有的商业伙伴 (3.26) 均为第三方，但并非所有的第三方都是商业伙伴。

3.28

利益冲突 conflict of interest

一种情形，其中相关方拥有直接或间接的个人利益或组织利益，这些利益可能损害或干扰其以组织 (3.2) 的最佳利益为出发点公正地履行职责的能力。

注1：个人利益可能包括多种类型，如商业、财务、家庭、专业、宗教或政治利益。

注2：组织利益涉及的是组织或其部分（如团队或部门）的利益，而非个体的利益。

(来源: ISO 37009:—1), 3.14]

3.29

尽职调查 due diligence

进一步评估贿赂风险 (3.12) 的性质和程度的过程 (3.15), 帮助组织 (3.2) 就特定交易、项目、活动、商业伙伴 (3.25) 和人员 (3.24) 做出决策。

3.30

反贿赂文化 anti-bribery culture

存在于整个组织 (3.1) 中的价值观、道德观、信念和行为, 它们与组织的结构和控制系统相互作用, 产生有利于反贿赂方针 (3.10) 和反贿赂管理体系 (3.5) 的行为规范。

注1: 此术语改编自 ISO 37301:2021, 3.28 中的“合规文化”。

4 组织的环境

4.1 理解组织及其环境

组织应确定与其宗旨相关且影响其实现反贿赂管理体系预期结果的能力的外部 and 内部问题。这些问题包括但不限于以下因素:

- a) 组织的规模、结构和委托决策权限;
- b) 组织运营或预期运营的地点和行业领域;
- c) 组织活动和运营的性质、规模和复杂性;
- d) 组织的商业模式;
- e) 组织控制的实体以及控制组织的实体;
- f) 组织的商业伙伴;
- g) 与公职人员互动的性质和程度;
- h) 适用的法定、监管、合同和职业义务及职责。组织应确定气候变化是否为一个相关问题。

注: 如果组织直接或间接控制另一组织的管理, 则视为对该组织具有控制权 (见A.13)。

4.2 理解相关方的需求和期望

组织应确定:

- a) 与反贿赂管理体系有关的相关方;
- b) 这些相关方的相关要求;
- c) 将通过反贿赂管理体系处理哪些要求。

注1: 有关相关方可能提出与气候变化相关的要求。

注2：在识别相关方的要求时，组织可以区分强制性要求、非强制性期望以及对相关方的自愿承诺。

4.3 确定反贿赂管理体系的范围

组织应确定反贿赂管理体系的边界和适用性，以建立其范围。

在确定此范围时，组织应考虑：

- a) 4.1 中提及的外部 and 内部因素；
- b) 4.2 中提及的要求；
- c) 4.5 中提及的贿赂风险评估的结果。范围应作为成文信息予以提供。

注：见A.2以获取指导。

4.4 反贿赂管理体系

组织应按照本标准的要求，建立、实施、保持并持续改进反贿赂管理体系，包括所需的过程及其相互作用。

反贿赂管理体系应形成文件，并应包含旨在识别和评估贿赂风险，以及预防、检测和应对贿赂风险的措施。

注1：完全消除贿赂风险是不可能的，任何反贿赂管理体系都无法预防和检测出所有贿赂行为。

反贿赂管理体系应合理且相称，同时考虑到4.3中提及的因素。

注2：见A.3以获取指导。

4.5 贿赂风险评估

4.5.1 组织应按策划的时间间隔进行贿赂风险评估，这些评估应：

- a) 考虑到4.1中列出的因素，识别组织可以合理预见的贿赂风险；
- b) 分析、评估和确定已识别贿赂风险的优先级；
- c) 评价组织现有控制措施在缓解已评估贿赂风险方面的适宜性和有效性。

4.5.2 组织应建立评估其贿赂风险水平的准则，这些准则应考虑组织的政策和目标。

4.5.3 贿赂风险评估应：

- a) 按策划的时间间隔进行评审，以便根据组织定义的时间和频率，对变化和新信息进行适当评估；
- b) 在组织结构或活动发生重大变化时进行评审。

4.5.4 组织应保留成文信息，以证明已进行贿赂风险评估，并已用于设计或持续改进反贿赂管理体系。

注：见A.4以获取指导。

5 领导作用

5.1 领导作用和承诺

5.1.1 治理机构

当组织设有独立的治理机构时，该机构应通过以下方式展示其在反贿赂管理体系方面的领导作用和承诺：

- a) 批准组织的反贿赂方针；
- b) 确保组织的战略与反贿赂方针相一致；
- c) 按策划的时间间隔接收并评审有关组织反贿赂管理体系内容和运行情况的信息；
- d) 要求为反贿赂管理体系的有效运行分配和指定充分且适当的资源；
- e) 对最高管理者实施组织反贿赂管理体系的情况、预期结果及其有效性进行合理监督。

如果组织没有独立的治理机构，这些活动应由最高管理者执行。

有关治理机构和最高管理者岗位的更多指导，请参阅ISO 37000:2021，4.2.3。

5.1.2 最高管理者

最高管理者应通过以下方式证实其在反贿赂管理体系方面的领导作用和承诺：

- a) 确保制定反贿赂方针和反贿赂目标；
- b) 确保将反贿赂管理体系要求融入组织的业务过程；
- c) 确保可获得反贿赂管理体系所需的资源；
- d) 就反贿赂方针进行内部和外部沟通；
- e) 传达有效反贿赂管理和符合反贿赂管理体系要求的重要性；
- f) 确保反贿赂管理体系实现其预期结果；
- g) 指导和支持人员为反贿赂管理体系的有效性做出贡献；
- h) 在组织内部促进形成适当的反贿赂文化；
- i) 促进持续改进；
- j) 支持其他相关岗位在其职责范围内展示其在预防和检测贿赂方面的领导作用；
- k) 鼓励使用报告程序来提出对疑似和实际贿赂行为的疑虑（见 8.9）；

l) 确保报告人员不会因诚信报告或基于合理信念报告违反或疑似违反组织反贿赂方针或反贿赂管理体系的行为，或拒绝参与贿赂行为（即使此种拒绝可能导致组织失去业务）而遭受报复、歧视或纪律处分（除非个人参与了违规行为）（见 7.2.2.1 d））；

m) 按策划的时间间隔向治理机构报告反贿赂管理体系的内容和运行情况，以及关于严重或系统性贿赂行为的指控。

注1：本标准中的“业务”一词可广泛解释为与组织存在目的相关的活动。

注2：见 A.5 以获取指导。

5.1.3 反贿赂文化

组织应在组织内部各层次开发、保持并推广反贿赂文化。

治理机构、最高管理者和管理层应展现出对组织范围内所需共同行为和行为标准的积极、可见、一致且持续的承诺。

最高管理者应鼓励支持反贿赂方针和反贿赂管理体系的行为。同时，应预防和不容忍任何损害反贿赂原则的行为。

注：见A.5以获取指导。

5.2 反贿赂方针

最高管理者应制定反贿赂方针，该政策应：

- a) 禁止贿赂；
- b) 要求遵守适用于组织的反贿赂法律；
- c) 与组织的目的相适应；
- d) 为设定反贿赂目标提供框架；
- e) 包括满足适用要求的承诺；
- f) 鼓励在诚信或基于合理信念的基础上，自信且无惧报复地提出担忧；
- g) 包括对反贿赂管理体系持续改进的承诺；
- h) 解释反贿赂职能的权威性和独立性；
- i) 解释不遵守反贿赂方针的后果。

反贿赂方针应：

- 作为成文信息可供获取；
- 在组织内部进行沟通；
- 适当时，可供相关方获取；
- 传达给存在较高贿赂风险的商业伙伴。

5.3 岗位、职责和权限

5.3.1 总则

最高管理者应对反贿赂管理体系的实施和合规负总体责任。

最高管理者应确保相关岗位的职责和权限在组织内部得到分配和沟通。

各级管理人员应负责要求其部门或职能范围内应用并遵守反贿赂管理体系。

治理机构、最高管理者和所有其他人员应负责理解、遵守并应用与其在组织中的岗位相关的反贿赂管理体系。

2) 如何:

——将这些措施整合并实施到其反贿赂管理体系过程中;

——评价这些措施的有效性。

6.2 反贿赂目标及实现目标的策划

组织应在相关职能和层次上建立反贿赂目标。反贿赂目标应:

a) 与反贿赂方针保持一致;

b) 可测量 (如果可行);

c) 考虑适用的要求;

d) 得到监视;

e) 得到沟通;

f) 适时更新;

g) 作为成文信息可获得;

h) 可实现。

在策划如何实现其反贿赂目标时, 组织应确定:

——将要做什么;

——需要什么资源;

——谁将负责;

——目标何时实现;

——如何评价结果;

——谁将实施制裁或处罚。

6.3 变更的策划

当组织确定需要对反贿赂管理体系进行变更时, 应按策划的方式执行变更。

注: 见A. 20以获取指导。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进反贿赂管理体系所需的资源。

注: 见A. 7以获取指导。

7.2 能力

7.2.1 总则

组织应：

- a) 确定在其控制下从事影响反贿赂绩效工作的人员所必需的能力；
- b) 基于适当的教育、培训或经验，确保这些人员胜任的；
- c) 适用时，采取措施以获得所必需的能力，并评价所采取措施的有效性。

应保存适当的成文信息作为能力的证据。

注：适用的措施可以包括，例如：提供培训、指导、或重新分配人员或业务合作伙伴，或者聘用或签订合同聘用相同的人员。

7.2.2 聘用过程

7.2.2.1 对于其所有人员，组织应实施以下程序：

a) 聘用条件要求人员遵守反贿赂方针和反贿赂管理体系，并赋予组织在人员不遵守时对其进行纪律处分的权利；

b) 在聘用开始后的合理期限内，人员应收到反贿赂方针的副本或获得访问该政策的途径，并接受与该政策相关的培训；

c) 组织应制定程序，以便对违反反贿赂方针或反贿赂管理体系的人员采取适当的纪律行动；

d) 人员不会因以下原因遭受报复、歧视或纪律行动（如威胁、孤立、降级、阻止晋升、调动、解雇、欺凌、迫害或其他形式的骚扰）：

1) 拒绝参与或拒绝任何他们合理判断存在较高贿赂风险且组织未采取缓解措施的活动；或

2) 出于诚意或基于合理信念，提出或报告试图、实际或涉嫌贿赂或违反反贿赂方针或反贿赂管理体系的情况（除非该个人参与了违反行为）。

e) 人员应了解报告潜在和实际利益冲突的必要性。

注：见A.8以获取指导。

7.2.2.2 对于贿赂风险评估（见4.5）中确定的存在较高贿赂风险的所有职位以及反贿赂职能，组织应实施以下程序：

a) 在聘用人员之前，以及在组织调动或晋升人员之前，对他们进行尽职调查（见8.2），以在合理范围内确定聘用或重新部署他们是适当的，并且有合理理由相信他们将遵守反贿赂方针和反贿赂管理体系；

b) 按策划的时间间隔评审绩效奖金、绩效目标和其他薪酬激励要素，以验证是否已采取合理保障措施，防止它们鼓励贿赂；

c) 此类人员、最高管理者和治理机构应按与已识别的贿赂风险相称的计划间隔提交声明，确认他们遵守反贿赂方针和反贿赂管理体系。

注1：反贿赂合规声明可以独立存在，也可以是更广泛的合规声明过程的一部分。

注2：见 A.8 以获取指导。

7.3 意识

7.3.1 人员的意识

人员应知晓：

- a) 反贿赂方针、程序和反贿赂管理体系，以及他们遵守的职责；
- b) 他们对反贿赂管理体系有效性的贡献，包括改进反贿赂绩效和报告疑似贿赂行为的益处；
- c) 不符合反贿赂管理体系要求的后果；
- d) 反贿赂程序和反贿赂管理体系，以及他们遵守的职责；
- e) 报告疑似贿赂行为的好处；
- f) 他们如何以及向谁报告任何疑虑（见 8.9）。

组织应保留关于意识计划的成文信息，以及提供的时间和对象。

7.3.2 人员的培训

组织应为人员提供充分和适当的反贿赂培训。此类培训应适当考虑贿赂风险评估（见 4.5）的结果，并涵盖以下问题：

- a) 适用的政策和程序；
- b) 贿赂风险以及贿赂对他们和组织可能造成的损害；
- c) 在他们履行职责时可能发生贿赂的情况，以及如何识别这些情况；
- d) 如何识别和应对贿赂的索求或提供；
- e) 他们如何帮助预防和避免贿赂，并识别关键的贿赂风险指标；
- f) 有关可用培训和资源的信息。

组织应保留关于培训程序、培训内容以及提供的时间和对象的成文信息。

注：适用的行动可以包括，例如：为人员提供培训，对人员进行辅导、重新分配人员或商业伙伴，或聘用或签订合同。

7.3.3 商业伙伴的培训

考虑到已识别的贿赂风险（见 4.5），组织还应实施程序，为代表其行事或为其利益行事的商业伙伴提供反贿赂培训，这些商业伙伴可能对组织构成高于低风险的贿赂风险。这些程序应明确需要接受此类培训的商业伙伴、培训内容以及提供培训的方式。

对于需要接受此类培训的商业伙伴，组织应保留关于培训程序、培训内容以及提供的时间和对象的成文信息。

注：商业伙伴的培训要求可以通过合同或类似要求传达，并由组织、商业伙伴或为此目的指定的其他方实施。

7.3.4 意识和培训计划

应在人员入职时，以及组织确定的策划时间间隔内，根据其角色、所面临的贿赂风险以及任何变化的情况，为其提供反贿赂意识和培训。意识和培训计划应在必要的策划时间间隔内进行更新，以反映相关的新信息。

注：见A.9获取指南。

7.4 反贿赂沟通

7.4.1 组织应确定与反贿赂管理体系有关的内部和外部沟通，包括：

- a) 沟通什么；
- b) 何时沟通；
- c) 与谁沟通；
- d) 如何沟通；
- e) 谁来沟通；
- f) 所使用哪种的语言沟通。

7.4.2 反贿赂方针应以适当的语言提供给组织的所有人员和商业伙伴，并直接沟通给那些对组织构成高于低风险贿赂风险的人员和商业伙伴。此外，反贿赂方针应通过组织的内部和外部沟通渠道适当地进行公布。

7.5 成文信息

7.5.1 总则

组织的反贿赂管理体系应包括：

- a) 本标准所要求的成文信息；
- b) 组织确定为反贿赂管理体系有效性所必需的成文信息。

注1：由于以下原因，不同组织的反贿赂管理体系所需成文信息的程度可能有所不同：

- 组织的规模及其活动、过程、产品和服务的类型；
- 过程的复杂性及其相互作用；
- 人员的胜任能力。

注2：成文信息可以作为反贿赂管理体系的一部分单独保留，也可以作为其他管理体系（如合规、财务、商业、审核）的一部分保留。

注3：见A.17获取指南。

7.5.2 成文信息创建和更新

在创建和更新成文信息时，组织应确保：

- a) 标识和说明（如标题、日期、作者、索引编号）；

-
- b) 形式（如语言、软件版本、图表）和载体（如纸质的、电子的）；
 - c) 评审和批准，以保持适宜性和充分性。

7.5.3 成文信息的控制

反贿赂管理体系和本标准所要求的成文信息应得到控制，以确保：

- a) 在需要的场合和时机，均可获得并适用；
- b) 予以妥善保护（如：防止泄密、不当使用或缺失）。

为了控制成文信息，组织应适用时处理以下活动：

- a) 分发、访问、检索和使用；
- b) 存储和防护，包括保持可读性；
- c) 更改控制（如版本控制）；
- d) 保留和处置。

对于组织所确定的策划和运行反贿赂管理体系所必需的来自外部的成文信息，组织应进行适当识别，并予以控制。

注：对于成文信息的“访问”可能意味着仅允许查阅或者意味着允许查阅和并授权修改。

8 运行

8.1 运行的策划和控制

组织应策划、实施和控制满足要求以及实施第6条所确定措施所需的过程，通过：

- a) 确定过程准则；
- b) 按照准则控制过程。

应提供必要的成文信息，以确信过程已按策划进行。

组织应控制计划内的变更，并评审非预期变更的后果，必要时采取措施减轻任何不利影响。

组织应确保对反贿赂管理体系相关的外部提供的过程、产品或服务进行控制。

这些过程应包括8.2至8.10中所述的具体控制。

注：外部组织处于管理体系范围之外，尽管外部提供的职能或过程在范围之内。

8.2 尽职调查

当组织的贿赂风险评估确定以下方面存在高于低风险的贿赂风险时：

- a) 特定类别的交易、项目或活动；
- b) 与特定类别商业伙伴的计划或正在进行的关系；或
- c) 特定职位的特定类别人员（见7.2.2.2）。

组织应评估这些类别中的特定交易、项目、活动、商业伙伴和人员的贿赂风险的性质和程度。此评估应包括任何必要的尽职调查，以获取足够信息来评估贿赂风险。尽职调查应按规定的频率更新，以便适当考虑变化和新信息。

注1：组织可以得出结论，认为对某些类别的人员和商业伙伴进行尽职调查是不必要的、不合理的或不成比例的。

注2：上述 a)、b) 和 c) 中列出的因素并非穷尽。

注3：见 A.10 获取指南。

8.3 财务控制

组织应实施管理贿赂风险的财务控制。

注：见A.11获取指南。

8.4 非财务控制

组织应实施管理采购、运营、销售、商业、人力资源、法律、并购和监管活动等方面贿赂风险的非财务控制。

注1：任何特定交易、活动或关系均可同时受财务控制和非财务控制。

注2：见 A.12 获取指南。

8.5 受控组织和商业伙伴实施反贿赂控制

8.5.1 组织应实施程序，要求其所有控制下的其他组织：

- a) 实施组织的反贿赂管理体系；或
- b) 实施其自身的反贿赂控制。

在每种情况下，仅在受控组织所面临的贿赂风险方面合理且相称的范围内实施，同时考虑按照4.5进行的贿赂风险评估。注：如果组织直接或间接控制另一组织的管理，则该组织对另一组织拥有控制权（见A.13）。

8.5.2 对于组织未控制的商业伙伴，若贿赂风险评估（见4.5）或尽职调查（见8.2）确定存在高于低风险的贿赂风险，且商业伙伴实施的反贿赂控制有助于减轻相关贿赂风险，组织应实施以下程序：

- a) 组织应确定商业伙伴是否已实施管理相关贿赂风险的反贿赂控制；
- b) 若商业伙伴未实施反贿赂控制，或无法验证其是否已实施。

在可行的情况下，组织应要求商业伙伴就相关交易、项目或活动实施反贿赂控制；或

若要求商业伙伴实施反贿赂控制不可行，则应在评估与该商业伙伴关系的贿赂风险（见4.5和8.2）以及组织管理此类风险的方式（见8.3、8.4和8.5）时将此作为考虑因素。

注：见A.13获取指南。

8.6 反贿赂承诺

对于存在高于低风险贿赂风险的商业伙伴，组织应实施程序，要求尽可能：

a) 商业伙伴承诺防止在相关交易、项目、活动或关系中，为商业伙伴自身、代表商业伙伴或为了商业伙伴的利益而进行的贿赂；

b) 若商业伙伴在相关交易、项目、活动或关系中，为自身、代表自身或为了自身的利益进行贿赂，组织有权终止与该商业伙伴的关系。

若无法满足上述a)或b)的要求，则应在评估与该商业伙伴关系的贿赂风险（见4.5和8.2）以及组织管理此类风险的方式（见8.3、8.4和8.5）时将此作为考虑因素。

注：见A.14获取指南。

8.7 礼品、招待、捐赠及类似利益

组织应实施程序，旨在防止提供、给予或接受礼品、招待、捐赠及类似利益，当这些行为被合理认为构成贿赂时。

注：见A.15获取指南。

8.8 管理反贿赂控制的不足

当对与商业伙伴的特定交易、项目、活动或关系进行的尽职调查（见8.2）表明，现有反贿赂控制无法管理贿赂风险，且组织无法或不愿实施额外或增强的反贿赂控制，或采取其他适当步骤（如改变交易、项目、活动或关系的性质）以使组织能够管理相关贿赂风险时，组织应：

a) 对于现有的交易、项目、活动或关系，根据贿赂风险和交易、项目、活动或关系的性质，采取适当步骤尽快终止、停止、暂停或撤出；

b) 对于拟议的新交易、项目、活动或关系，推迟或拒绝继续进行。

8.9 提出疑虑

组织应实施以下程序：

a) 鼓励并允许人员基于诚意或合理信念，向反贿赂职能部门或适当人员（直接或通过适当的第三方）报告企图、怀疑和实际的贿赂行为，或反贿赂管理体系中的任何违反或薄弱环节；

b) 除为推进调查所必需的范围外，要求组织对报告保密，以保护报告者的身份以及报告中涉及或提及的其他人员的身份；

c) 允许匿名报告；

d) 禁止报复，并保护那些基于诚意或合理信念提出或报告关于企图、实际或怀疑的贿赂行为，或违反反贿赂方针或反贿赂管理体系的疑虑的人员免受报复；

e) 使人员能够从适当人员那里获得关于在面对可能涉及贿赂的疑虑或情况时该如何做的建议。

组织应确保所有人员都了解报告程序，能够使用这些程序，并了解他们在这些程序下的权利和保护。

注1：这些程序可以与用于报告其他疑虑问题（如安全、渎职、不法行为或其他严重风险）的程序相同，或作为其一部分。

注2：组织可以委托商业伙伴代表其管理报告系统。

注3：在某些司法管辖区，上述 b)和 c)项的要求被法律禁止。在这些情况下，组织应记录其无法遵守的情况。

注4：有关进一步指导，请见 ISO 37002。

8.10 调查和处理贿赂

组织应实施以下程序：

a) 要求对任何被报告、发现或有合理理由怀疑的贿赂行为，或违反反贿赂方针或反贿赂管理体系的行为进行评估，并在适当时进行调查；

b) 要求在调查揭示出任何贿赂行为或违反反贿赂方针或反贿赂管理体系的行为时，采取适当行动；

c) 赋予调查人员权力并使其能够进行调查；

d) 要求相关人员在调查中予以合作；

e) 要求向反贿赂职能部门和其他适当的合规职能部门报告调查的状态和结果；

f) 要求调查保密，并确保调查结果是保密的。

调查应由不属于被调查角色或职能的人员进行，并向其报告。组织可以任命商业伙伴进行调查，并向不属于被调查角色或职能的人员报告结果。

注1：有关指导，请见 A.18。

注2：在某些司法管辖区，上述 f)项的要求被法律禁止。在这种情况下，组织应记录其无法遵守的情况。

注3：有关进一步指导，见 ISO/TS 37008。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a) 需要监视和测量什么；

b) 需要什么方法进行监视、测量、分析和评价，以确保结果有效；

c) 何时实施监视和测量；

d) 何时对监视和测量的结果进行分析和评价。

组织应保留适当的成文信息，以作为结果的证据。

组织应评价反贿赂绩效和反贿赂管理体系的有效性。

注：有关指导，请见A.19。

9.2 内部审核

9.2.1 总则

组织应按策划的时间间隔进行内部审核，以提供关于反贿赂管理体系是否：

- a) 是否符合：
 - 1) 组织自身的反贿赂管理体系要求；
 - 2) 本标准的要求。

- b) 是否得到有效的实施和保持。

注1：ISO 19011 提供了关于管理体系审核的指导。

注2：组织内部审核活动的范围和规模可能因多种因素而异，包括组织规模、结构、成熟度和地点。

注3：有关指导，请见 A.16。

9.2.2 内部审核方案

组织应策划、建立、实施和保持一个或多个审核方案，包括频率、方法、职责、策划要求和报告。

在建立内部审核方案时，组织应考虑相关过程的重要性和以往审核的结果。

组织应：

- a) 规定每次审核的审核目标、准则和范围；
 - b) 选择审核员并进行审核，以确保审核过程的客观性和公正性；
 - c) 确保审核结果报告给相关管理者、反贿赂职能部门、最高管理者，以及适当时，治理机构。
- 应保留成文信息作为审核方案实施和审核结果的证据。

9.2.3 审核程序、控制和系统

这些审核应合理、适当并基于风险。此类审核应包括内部审核过程或其他评审程序、控制和系统的程序，以评审：

- a) 贿赂或怀疑贿赂；
- b) 违反反贿赂方针或反贿赂管理体系；
- c) 商业伙伴未符合组织适用的反贿赂要求；
- d) 反贿赂管理体系中的薄弱环节或改进机会。

9.2.4 客观性和公正性

为确保这些审核方案的客观性和公正性，组织应确保这些审核由以下之一进行：

- a) 为此过程建立或任命的独立职能或人员；或

b) 反贿赂职能部门，除非审核范围包括对反贿赂管理体系本身的评价，或反贿赂职能部门负责的其他类似工作；或

c) 来自被审核部门或职能以外的其他部门或职能的适当人员；或

d) 适当的第三方；或

e) 由a)至d)中任何一项组成的组合。

组织应确保没有审核员审核其自己的工作领域。

9.3 管理评审

9.3.1 总则

最高管理者应按策划的时间间隔评审组织的反贿赂管理体系，以确保其持续的适宜性、充分性和有效性。

治理机构应基于最高管理者和反贿赂职能部门提供的信息，以及治理机构要求或获取的任何其他信息，按计划的时间间隔对最高管理者实施反贿赂管理体系的情况进行评审。

9.3.2 管理评审输入

管理评审应包括：

- a) 以往管理评审所采取措施的状况；
- b) 与反贿赂管理体系有关的外部 and 内部因素的变化；
- c) 与反贿赂管理体系有关的相关方需求和期望的变化；
- d) 反贿赂管理体系绩效的信息，包括以下趋势：
 - 1) 不合格和纠正措施；
 - 2) 监视和测量结果；
 - 3) 审核结果；
 - 4) 贿赂报告；
 - 5) 调查；
 - 6) 组织面临的贿赂风险的性质和程度；
- e) 持续改进的机会；
- f) 针对贿赂风险所采取措施的有效性。

9.3.3 管理评审结果

管理评审的结果应包括与持续改进机会以及反贿赂管理体系任何变更需求相关的决定。

应保留成文信息作为管理评审结果的证据。

应向治理机构报告最高管理者评审结果的摘要。

9.4 反贿赂职能部门的评审

反贿赂职能部门应持续评估反贿赂管理体系是否：

- a) 充分，以有效管理组织面临的贿赂风险；
- b) 得到了有效实施。

反贿赂职能部门应按计划的时间间隔，并在适当时临时向治理机构和最高管理者，或向治理机构或最高管理者的适宜委员会，报告反贿赂管理体系的充分性和实施情况，包括调查和审核的结果。

注1：此类报告的频率取决于组织的结构和需求。

注2：组织可以利用商业伙伴协助进行评审，只要将商业伙伴的意见适当地传达给反贿赂职能部门、最高管理者，以及适当时的治理机构。

10 改进

10.1 持续改进

组织应持续改进反贿赂管理体系的适宜性、充分性和有效性。

注：见A.20获取指导。

10.2 不合格和纠正措施

当发生不合格时，组织应：

- a) 对不合格作出反应，并适用时：
 - 1) 采取措施予以控制和纠正；
 - 2) 处置后果。
- b) 通过以下方式评价消除不合格原因的措施需求，以防止其再次发生或在其他地方发生：
 - 1) 评审不合格；
 - 2) 确定不合格的原因；
 - 3) 确定是否存在或可能发生类似的不合格；
 - a) 实施任何所需的措施；
 - b) 评审所采取的任何纠正措施的有效性；
 - c) 必要时，对反贿赂管理体系作出变更。

纠正措施应与所遇到的不合格的影响程度相适应。应保留成文信息作为以下方面的证据：

不合格的性质以及随后所采取的任何措施；

任何纠正措施的结果。

注：见A.20获取指导。



附录 A (资料性) 本标准使用指南

A.1 总则

本附录中的指南仅为示例。其目的是在某些特定领域指明组织在实施其反贿赂管理体系时可采取的行动类型。本指南既非旨在全面详尽，亦非规定性要求，组织无需实施以下步骤即可拥有一个符合本标准要求的反贿赂管理体系。组织所采取的步骤应针对其面临的贿赂风险的性质和程度而言是合理且相称的（见4.5，以及4.1和4.2中的因素）。

有关反贿赂管理的良好实践的进一步指南，请参见参考文献中列出的出版物。

A.2 反贿赂管理体系的范围

A.2.1 独立或整合的反贿赂管理体系

组织可以选择将此反贿赂管理体系作为单独的系统实施，或作为整体合规管理体系的组成部分（在此情况下，组织可参考ISO 37301获取指南）来实施。组织还可以选择将此反贿赂管理体系与其其他管理体系（如质量、环境和信息安全管理体系，此时组织可参考ISO 9001、ISO 14001和ISO/IEC 27001）以及ISO 26000和ISO 31000并行实施或作为其一部分来实施。

A.2.2 便利支付和勒索支付

A.2.2.1 便利支付有时指的是为获取服务而进行的非法或非正式支付，而支付者本有权在不支付此类费用的情况下合法获得这些服务。它通常是指为公共官员或具有认证职能的人员支付的一笔相对较小的费用，以确保或加快常规或必要行动（如签发签证、工作许可、海关清关或安装电话）的执行。尽管便利支付通常被视为与例如为赢得业务而支付的贿赂在性质上不同，但在大多数地区，它们是非法的，并且在本标准中被视为贿赂，因此应被组织的反贿赂管理体系所禁止。

A.2.2.2 勒索支付是指因对人员健康、安全或自由的实际或感知威胁而强行从人员那里提取金钱，这超出了本标准的范围。个人的安全和自由至关重要，许多法律体系不将因合理担心自己或他人健康、安全或自由而支付金钱的行为定为犯罪。组织可以制定政策，允许在人员担心自己或他人的健康、安全或自由而面临迫在眉睫的危险时支付金钱。

A.2.2.3 组织应向可能面临此类支付要求或索求的任何人员提供具体指导，说明如何避免和处理这些情况。此类指导可以包括，例如：

a) 规定面临支付要求时任何人员应采取的行动；

1) 在便利支付的情况下，要求提供支付合法的证明以及官方支付收据，如果没有令人满意的证明，则拒绝支付；

2) 在勒索支付的情况下，如果其健康、安全或自由，或他人的健康、安全或自由受到威胁，则进行支付；

b) 规定进行了便利支付或勒索支付的人员应采取的行动：

1) 记录事件；

2) 向适当的经理或反贿赂职能部门报告事件；

c) 规定当人员进行了便利支付或勒索支付时组织应采取的行动：

1) 指定适当的经理调查事件（最好是反贿赂职能部门或与人员所在部门或职能无关的经理）；

2) 在组织的账户中正确记录支付；

3) 如果适当或法律要求，向相关当局报告支付。

A.3 反贿赂管理体系

A.3.1 贿赂通常具有隐蔽性，难以预防、发现和应对。认识到这些困难，本标准的总体意图是，组织的治理机构和最高管理者层：

——对预防、发现和应对与组织业务或活动相关的贿赂做出真正承诺；

——本着真诚的意图，在组织中实施旨在预防、发现和应对贿赂的措施。

A.3.2 这些措施不能过于昂贵、繁琐和官僚，以至于组织无法承担或使业务停滞，同时也不能过于简单和无效，以至于贿赂轻易发生。措施需要与贿赂风险相适应，并应在其预防、发现和应对贿赂的目标上有合理的成功机会。

A.3.3 虽然需要实施的反贿赂措施类型在国际良好实践中得到了相当广泛的认可，并且其中一些在本标准中作为要求体现，但根据相关情况，需要实施的具体措施细节差异很大。无法详细规定组织在任何特定情况下应该做什么。因此，本标准中引入了“合理且相称”的限定条件，以便根据每种情况的自身特点进行判断。

A.3.4 以下示例提供了一些指导，说明在不同情况下如何应用“合理且相称”的限定条件：

a) 一个大型跨国公司需要处理多层管理层和数千名员工。其反贿赂管理体系通常需要比只有少数员工的小型组织更为详细。

b) 在贿赂风险较高的地点开展活动的组织，通常需要比仅在贿赂风险较低的地点（贿赂相对较少发生）开展活动的组织，进行更为全面的贿赂风险评估和尽职调查程序，并对该地点的业务交易实施更高水平的反贿赂控制。

c) 尽管许多交易或活动都存在贿赂风险，但参与大型、高价值交易或涉及广泛商业伙伴的活动的组织所实施的贿赂风险评估、尽职调查程序和反贿赂控制，可能比涉及向多个客户销售小价值物品或与单一方进行多个较小交易的业务所实施的控制更为全面。

d) 业务伙伴范围非常广泛的组织可以在其贿赂风险评估中得出结论，认为某些类别的业务伙伴（如零售客户）不太可能构成超过低风险的贿赂风险，并在设计和实施其反贿赂管理体系时考虑到这一点。例如，对于从组织购买消费品等物品的零售客户，尽职调查不太可能是必要的，或作为相称且合理的控制。

A.3.5 尽管许多交易都存在贿赂风险，但组织应对高风险贿赂交易实施比低风险贿赂交易更为全面的反贿赂控制。在此背景下，重要的是要理解，识别和接受低贿赂风险并不意味着组织接受贿赂发生的事实，即贿赂发生的风险（贿赂是否可能发生）与贿赂的发生（贿赂本身的事实）并不相同。组织可以在对贿赂发生持“零容忍”态度的同时，仍在贿赂风险低或高于低风险的情况下开展业务（只要应用了充分的缓解措施）。下面提供了关于具体控制的进一步指导。

A.4 贿赂风险评估

A.4.1 4.5所要求的贿赂风险评估旨在使组织为其反贿赂管理体系奠定坚实基础。此评估用于识别管理体系将重点关注的贿赂风险，即组织认为需优先进行贿赂风险缓解、控制实施以及分配反贿赂合规人员、资源和活动的贿赂风险。组织如何开展贿赂风险评估、采用何种方法、如何权衡和确定贿赂风险的优先级，以及接受（即“风险承受力”）或容忍的贿赂风险水平，均由组织自行决定。特别是，组织应制定其评估贿赂风险的标准（例如，风险是“低”、“中”还是“高”）；然而，在此过程中，组织应考虑其反贿赂方针和目标。

A.4.2 以下是一个组织如何选择进行此评估的示例。

a) 选择贿赂风险评估准则。例如，组织可以选择三级标准（如“低”、“中”、“高”）、更详细的五级或七级准则，或采用更详细的方法。这些准则通常会考虑多个因素，包括贿赂风险的性质、贿赂发生的可能性，以及一旦发生贿赂，其后果的严重性；

b) 评估组织的规模和结构所带来的贿赂风险。一个位于单一地点、管理控制权集中于少数人的小型组织，比一个在多个地点运营、结构分散的大型组织更容易控制其贿赂风险；

c) 评审组织当前运营或预期运营的地点和部门，并评估这些地点和部门可能带来的贿赂风险水平。可使用适当的贿赂指数来协助此评估。组织可将贿赂风险较高的地点或部门视为“中”或“高”风险，例如，这可能导致组织对这些地点或部门中的活动实施更高水平的控制；

d) 评审组织活动和运营的性质、规模和复杂性。

1) 例如，与在多个地点参与众多大型建设项目的组织相比，在一个地点进行小型制造运营的组织可能更容易控制贿赂风险；

2) 某些活动可能带来特定的贿赂风险，例如抵消安排，即政府采购产品或服务时要求供方将合同价值的一定比例再投资于采购国。组织应采取适当步骤，防止抵消安排构成贿赂。

e) 按类别评审组织的现有和潜在商业伙伴类型，并原则上评估其带来的贿赂风险。例如：

1) 组织可能拥有大量客户，他们从组织购买价值很低的产品，实际上对组织构成极小的贿赂风险。在这种情况下，组织可能认为这些客户的贿赂风险较低，并确定无需对这些客户实施任何特定的反贿赂控制。或者，组织可能与从组织购买价值极高产品的客户打交道，这些客户可能带来显著的贿赂风险[例如，要求组织提供贿赂以换取付款、审批的风险]。这些类型的客户可被视为“中”或“高”贿赂风险，组织需对他们实施更高水平的反贿赂控制；

2) 不同类别的供方可能带来不同水平的贿赂风险。例如，工作范围非常广泛的供方，或与组织的客户、客户或相关公职人员有接触的供方，可能带来“中”或“高”贿赂风险。某些类别的供方可能风险“低”，例如位于贿赂风险较低地点的供方，且与交易或组织的客户或客户相关的公职人员无接触。某些类别的供方可能带来“极低”贿赂风险，例如提供少量低价值物品的供方、机票或酒店在线购买服务。组织可得出结论，无需对这些低或极低贿赂风险的供方实施特定的反贿赂控制。

3) 代表组织与组织的客户或公职人员互动的代理人或中介可能带来“中”或“高”贿赂风险，特别是如果他们按佣金或成功费计费。

f) 评审可能与带来贿赂风险的国内或国外公职人员互动的性质和频率，例如，与负责颁发许可和审批的公职人员互动可能带来贿赂风险；

g) 评审适用的法定、监管、合同和职业义务与职责，例如禁止或限制款待公职人员或使用代理人。

h) 考虑组织能够在多大程度上影响或控制所评估的风险。

A.4.3 上述贿赂风险因素相互关联。例如，同一类别的供方根据其运营地点的不同，可能带来不同的贿赂风险。

A.4.4 在评估了相关贿赂风险后，组织可以确定针对每个风险类别所应用的反贿赂控制的类型和水平，并评估现有控制是否充分。如果不充分，可以适当地改进控制。例如，可能对贿赂风险较高的地点和商业伙伴类别实施更高水平的控制。组织可以确定，对低贿赂风险活动或商业伙伴实施低水平控制是可以接受的。本标准中的某些要求明确排除了将这些要求应用于低贿赂风险活动或商业伙伴的必要性（尽管组织如果愿意，可以选择应用它们）。

A.4.5 组织可以改变交易、项目、活动或关系的性质，从而将贿赂风险的性质和程度降低到现有、增强或额外的反贿赂控制能够充分管理的水平。

A.4.6 此贿赂风险评估工作并非旨在成为一项广泛或过于复杂的工作，且评估结果不一定正确（例如，被评估为低贿赂风险的交易可能最终涉及贿赂）。在合理可行的范围内，贿赂风险评估的结果应反映组织面临的实际贿赂风险。该工作应设计为一种工具，帮助组织评估和确定其贿赂风险的优先级，并应按计划间隔进行评审，并根据组织或环境的变化（如新市场或产品、法律要求、获得的经验）进行修订。

注：ISO 31000和ISO 31022提供了进一步的指导。

A.5 管理机构和最高管理者的职责

A.5.1 总则

A.5.1.1 许多组织都设有某种形式的管理机构（例如董事会或监事会），负责组织的总体监督职责。这些职责包括对组织反贿赂管理体系的监督。然而，管理机构通常不对组织的日常活动进行直接指导。这是最高管理者人员（例如首席执行官、首席运营官）的职责，在本标准中称为“最高管理者”。关于反贿赂管理体系，管理机构应了解其内容和运行方式，并应对管理体系的充分性、有效性和实施情况进行合理监督。它应通过管理评审过程，在计划的时间间隔内接收有关管理体系性能的信息（这可以是向整个管理机构，或其下属委员会，如审计委员会报告）。在这方面，反贿赂职能应能够直接向管理机构（或其适当的委员会）报告有关管理体系的信息。

A.5.1.2 有些组织，特别是较小的组织，可能没有单独的管理机构，或者管理机构和最高管理者的职责合并在一个团体甚至一个人身上。在这种情况下，该团体或个人将承担本标准分配给最高管理者和管理机构的责任。

注：领导层的承诺有时被称为“高层的基调”或“来自高层的基调”。

A.5.2 反贿赂文化

A.5.2.1 支持反贿赂文化发展的因素包括：

- 管理层积极实施、推广并明显遵守组织的反贿赂文化；
- 通过树立榜样和领导作用，强调组织反贿赂文化的重要性；
- 在员工入职计划中强调组织的反贿赂文化；
- 与员工就组织的反贿赂文化进行持续沟通；
- 对员工在推广组织反贿赂文化方面的成就给予明显认可；
- 对损害组织反贿赂文化的员工行为采取一致的处理方式，无论其职位如何。

A.5.2.2 反贿赂文化的证据体现在以下方面的程度：

- 上述各项是否得到记录、实施和实践；

-
- 员工相信上述各项已得到实施；
 - 员工理解组织反贿赂文化与其职位、自身活动及其业务部门的相关性；
 - 员工重视反贿赂管理体系的作用和目标，特别是反贿赂方针、相关程序以及反贿赂职能的价值；
 - 针对损害组织反贿赂管理体系的员工行为所采取的纠正措施，在组织的所有适当层级上得到“认可”并按要求执行。

A.6 反贿赂职能

A.6.1 反贿赂职能的人员配置

反贿赂职能的人员数量取决于多种因素，如组织的规模、组织面临的贿赂风险程度以及由此产生的工作负荷。在小型组织中，反贿赂职能可能由一人兼职负责，该人员会将这一职责与其他职责相结合。当贿赂风险程度和工作负荷足以证明其必要性时，反贿赂职能可以由一人全职负责。在大型组织中，该职能可能由多人负责。一些组织可以将责任分配给具备一系列相关专业知识的委员会。一些组织可以选择由第三方承担部分或全部反贿赂职能，这是可以接受的，但前提是组织内的适当管理人员需保留对反贿赂职能的总体职责和权限，并监督第三方提供的服务。

A.6.2 反贿赂职能人员的资质要求

本标准要求反贿赂职能由具备适当能力、地位、权力和独立性的人员负责。在这方面：

- a) “能力”指相关人员具备适当的教育、培训或经验，具备处理角色要求的个人能力，以及学习和适当履行角色的能力；
- b) “地位”指其他人员可能倾听并尊重被赋予合规责任的人员的意见；
- c) “权力”指被赋予合规责任的相关人员由治理机构和高层管理授予足够的权力，以便能够有效履行合规职责；
- d) “独立性”指被赋予合规责任的相关人员尽可能不亲自参与组织内可能面临贿赂风险的活动。当组织任命全职人员负责该角色时，这一点更容易实现，但对于任命人员将合规角色与其他职能相结合的小型组织来说则更为困难。当反贿赂职能为兼职时，该角色不应由在执行其主要职能时可能接触贿赂的个人担任。在非常小的组织中，如果难以实现独立性，适当的人员应尽其所能将其其他职责与合规职责分开，以保持公正。

A.6.3 反贿赂职能的直接沟通渠道

反贿赂职能必须能够直接与高层管理和治理机构沟通相关信息。该职能不应仅向链条中的另一位经理报告，然后该经理再向高层管理报告，因为这会增加反贿赂职能所传递的信息未被高层管理充分或清晰接收的风险。反贿赂职能还应与治理机构建立直接的沟通关系，而无需通过高层管理。这可以直接与完整的治理机构（如董事会或监督委员会）沟通，也可以与治理机构或高层管理特别委托的委员会（如审计或伦理委员会）沟通。

A.6.4 反贿赂职能的主要责任

反贿赂职能的主要责任是监督反贿赂管理体系的设计和实施。这不应与对组织反贿赂绩效和遵守适用反贿赂法律的直接责任相混淆。每个人都有责任以道德和合规的方式行事，包括遵守组织反贿赂管理体系和反贿赂法律的要求。特别重要的是，管理层应在其负责的组织部分中发挥领导作用，以实现合规。

注：ISO 37301 提供了进一步的指导。

A.7 资源

所需资源取决于多种因素，如组织的规模、其业务的性质以及所面临的贿赂风险。资源示例包括以下内容：

- a) 人力资源：应有足够的人员，他们能够投入足够的时间履行其相关的反贿赂职责，以确保反贿赂管理体系能够有效运行。这包括为反贿赂职能分配足够的人员（无论是内部还是外部人员）。
- b) 物质资源：组织内，包括反贿赂职能部门，应有必要的物质资源，以确保反贿赂管理体系能够有效运行，例如办公空间、家具、计算机硬件和软件、培训材料、电话、文具等；
- c) 财务资源：应有足够的预算，包括反贿赂职能部门的预算，以确保反贿赂管理体系能够有效运行。

A.8 聘用程序

A.8.1 对人员的尽职调查

在任命人员之前对其进行尽职调查时，组织应根据拟任人员的职能和相应的贿赂风险，采取以下行动：

- a) 在面试时与潜在人员讨论组织的反贿赂方针，并形成他们是否似乎理解并接受合规重要性的看法；
- b) 采取合理步骤核实潜在人员的资格准确无误；
- c) 采取合理步骤从潜在人员的前雇主那里获得令人满意的推荐信；
- d) 采取合理步骤确定潜在人员是否曾涉及贿赂行为；
- e) 采取合理步骤核实组织并非因为潜在人员在之前的工作中不当偏袒组织而向其提供聘用机会；
- f) 核实向潜在人员提供聘用机会的目的并非为了为组织获取不当的有利待遇；
- g) 采取合理步骤识别潜在人员与公职人员的关系。

A. 8.2 绩效奖金

A. 8.2.1 包括奖金和激励在内的薪酬安排，即使是无意的，也可能鼓励人员参与贿赂。例如，如果经理因为为组织赢得合同而获得奖金，该经理可能会受到诱惑去支付贿赂，或者对代理人或合资伙伴支付贿赂视而不见，以确保赢得合同。如果对经理施加过大的业绩压力（例如，如果经理因未达到过高的销售目标而被解雇），也可能产生同样的结果。组织需要密切关注这些薪酬方面，以确保在合理范围内它们不会成为贿赂的诱因。

A. 8.2.2 人员评价、晋升、奖金和其他奖励可以作为激励，鼓励人员按照组织的反贿赂方针和反贿赂管理体系行事。然而，组织在这种情况下需要谨慎，因为失去奖金等的威胁可能导致人员隐瞒反贿赂管理体系中的失败。

A. 8.2.3 应使人员意识到，违反反贿赂管理体系以提高其在其他领域（如实现销售目标）的绩效评级是不可接受的，并应导致采取纠正和/或纪律行动。

A. 8.3 利益冲突

A. 8.3.1 组织应识别、分析和评价内部和外部利益冲突的风险。组织应明确告知所有人员，他们有义务报告任何潜在和实际的利益冲突，如与他们的工作直接或间接相关的家庭、财务或其他联系。这有助于组织识别人员可能促成或未能防止或报告贿赂的情况，例如：

a) 当组织的销售经理与客户的采购经理有关联时；

b) 当采购职能的经理在供方中持有财务利益时；

c) 当组织的直线经理在竞争对手的业务中有个人财务利益时；

d) 当组织的董事（可能担任非执行职务）或最高管理者在竞争组织或潜在收购组织中拥有合法或隐蔽的个人利益或职位时。

A. 8.3.2 组织应记录所有利益冲突声明，以及实际或潜在利益冲突的任何情况，以及是否以及采取了哪些行动来缓解冲突。

A. 8.3.3 这些（规定/政策）应至少每年评审一次，以确保其仍然相关且是最新的。

A. 8.4 组织人员的贿赂

A. 8.4.1 为防止、检测和应对组织人员代表组织贿赂他人（“对外贿赂”）的风险所采取的必要措施，可能与用于防止、检测和应对贿赂组织人员（“对内贿赂”）的风险的措施不同。例如，识别和减轻对内贿赂风险的能力可能会受到组织无法控制的信息（如员工个人银行账户和信用卡交易数据）、适用法律（如隐私法）或其他因素的显著限制。因此，组织可用于减轻对外贿赂风险的控制措施的数量和类型可能超过其能够实施以减轻对内贿赂风险的控制措施的数量。

A. 8. 4. 2 组织人员的贿赂最有可能发生在那些能够代表组织做出决策或影响决策的人员身上（例如，能够授予合同的采购经理；能够批准已完成工作的主管；能够任命人员或批准工资或奖金的经理；负责准备颁发许可证和执照文件的职员）。由于贿赂很可能被组织系统或控制范围之外的人员接受，因此组织防止或检测这些贿赂的能力可能有限。

A. 8. 4. 3 除了上述关于尽职调查和利益冲突段落中提到的步骤外，本标准中关于此风险的以下要求可以减轻对内贿赂的风险：

a)组织的反贿赂方针（见 5. 2）应明确禁止组织人员及代表组织工作的任何人索取和接受贿赂；

b)指导和培训材料（见 7. 3）应强化禁止索取和接受贿赂的规定，并包括：

1) 报告贿赂问题的指南（见 8. 9）；

2) 强调组织的无报复政策（见 8. 9）；

c)组织的礼品和款待政策（见 8. 7）应限制人员接受礼品和款待；

d)在组织网站上公布组织的反贿赂方针以及如何报告贿赂的详细信息，有助于与商业伙伴设定期望，从而降低商业伙伴提供贿赂或组织人员索取或接受贿赂的可能性；

e) 控制措施（见 8. 3 和 8. 4），例如要求使用经批准的供方、竞争性投标、合同授予、工作批准等至少需要两人签名，以减少腐败的授予、批准、支付或利益的风险。

A. 8. 4. 4 组织还可以实施审计程序，以识别人员如何利用现有控制弱点谋取私利。示例程序包括：

a) 评审工资单文件，查找虚假和重复的人员记录；

b) 评审人员业务费用记录，以识别异常支出；

c) 将人员工资单文件信息（如个人银行账户号码和地址）与组织供方主文件中的银行账户和地址信息进行比较，以识别潜在的利益冲突场景。

A. 8. 5 临时员工或工人

在某些情况下，临时员工或工人由劳务供方或其他商业伙伴提供给组织。在这种情况下，组织应确定这些临时员工或工人（如果有的话）所带来的贿赂风险是否通过将其视为自己的员工进行培训和控制而得到充分处理，或者是否通过提供临时员工或工人的商业伙伴施加适当的控制。

A. 9 意识与培训

A. 9. 1 培训目的

培训的目的是帮助相关人员根据其在组织内或与组织相关的角色，适当理解以下内容：

a) 他们及其组织面临的贿赂风险；

b) 反贿赂方针；

c) 与其角色相关的反贿赂管理体系的方面；

d) 他们需要采取的任何必要的预防和报告行动，以应对任何贿赂风险或疑似贿赂行为。

A. 9. 2 培训的形式和范围

培训的形式和范围取决于组织的规模和面临的贿赂风险。培训可以通过在线模块或面对面的方式进行（例如，课堂会议、研讨会、相关人员之间的圆桌讨论或一对一会议）。培训的方法不如其成果重要，即所有相关人员都应理解A. 9. 1中提及的问题。

A. 9. 3 面对面培训的建议

建议对治理机构以及任何参与具有较高贿赂风险的操作和流程的人员（无论其在组织内的职位或层级）和商业合作伙伴进行面对面培训。

A. 9. 4 反贿赂职能人员的培训

如果负责反贿赂职能的相关人员没有足够的相关经验，组织应提供必要的培训，使其能够充分履行反贿赂职能。

A. 9. 5 培训的组合方式

培训可以作为独立的反贿赂培训进行，也可以作为组织整体合规和道德培训或入职计划的一部分。

A. 9. 6 培训内容的适应性

培训内容可以根据人员的角色进行调整。在角色中不面临显著贿赂风险的人员可以接受关于组织政策的非常简单的培训，以便他们理解政策，并知道在发现潜在违规行为时应该怎么做。角色涉及高风险贿赂的人员应接受更详细的培训。

A. 9. 7 培训的重复性

培训应根据需要重复进行，以确保人员及时了解组织的政策和程序、与其角色相关的任何发展以及任何监管变化。

A. 9. 8 对商业合作伙伴的培训要求

将培训要求应用于根据7. 3. 4要求确定的商业合作伙伴，这提出了特别的挑战，因为此类商业合作伙伴的员工通常不直接为组织工作，且组织通常无法直接接触这些员工进行培训。为商业合作伙伴工作的员工的实际培训通常由商业合作伙伴或为此目的保留的其他方进行。重要的是，那些可能对组织构成较高贿赂风险的商业合作伙伴的员工应意识到这一问题，并接受合理旨在降低此风险的培训。7. 3. 4的内容要求组织至少识别出哪些商业合作伙伴的员工应接受反贿赂培训，此类培训的最小内容应是什么，以及应如何进行此类培训。培训本身可以由商业合作伙伴、指定的其他方提供，或者如果组织选择，也可以由组织自己提供。组织可以通过多种方式向其商业合作伙伴传达这些义务，包括作为合同安排的一部分。

A. 10 尽职调查

A. 10.1 尽职调查的目的

对某些交易、项目、活动、商业合作伙伴或组织人员进行尽职调查的目的是，进一步评估作为组织风险评估（见4.5）一部分所识别的、超出低风险的贿赂风险的范围、规模和性质。它还起到预防和检测贿赂风险的额外、有针对性的控制作用，并为组织决定是否推迟、终止或修改这些交易、项目或与商业合作伙伴或人员的关系提供信息。

A. 10.2 项目、交易和活动的尽职调查因素

对于项目、交易和活动，组织可能认为有用的评估因素包括：

- a) 结构、性质和复杂性（例如，直接或间接销售、折扣水平、合同授予和招标程序）；
- b) 融资和支付安排；
- c) 组织参与的范围和可用资源；
- d) 控制程度和可见性；
- e) 涉及的商业合作伙伴和其他第三方（包括公职人员）；
- f) 上述 e) 中任何一方与公职人员之间的联系；
- g) 涉及方的能力和资格；
- h) 客户的声誉；
- i) 地点；
- j) 市场或媒体上的报告。

这些因素有助于组织更全面地了解潜在的风险点，从而做出更加明智的决策。通过尽职调查，组织可以识别出可能存在的贿赂风险，并采取相应的措施来预防或减轻这些风险。

A. 10.3 对商业合作伙伴的尽职调查

a) 组织在评估商业合作伙伴时可能认为有用的因素包括：

- 1) 商业合作伙伴是否为合法商业实体，如通过公司注册文件、年度备案账目、税务识别号、证券交易所上市等指标证明；
- 2) 商业合作伙伴是否具备履行合同所需的资质、经验和资源；
- 3) 商业合作伙伴是否建立了反贿赂管理体系，以及该体系的完善程度；
- 4) 商业合作伙伴是否有贿赂、欺诈、不诚实或类似不当行为的声誉，或是否曾因贿赂或类似犯罪行为被调查、定罪、制裁或禁止参与；
- 5) 商业合作伙伴的股东（包括最终实益所有人）和最高管理者的身份，以及他们；

6) 是否有贿赂、欺诈、不诚实或类似不当行为的声誉；

7) 是否曾因贿赂或类似犯罪行为被调查、定罪、制裁或禁止参与；

8) 是否与组织的客户或相关公职人员有直接或间接的联系，这可能导致贿赂（这包括本身不是公职人员，但可能与公职人员、公职候选人等有直接或间接关系的人）；

9) 交易结构和支付安排。

b) 尽职调查的性质、类型和范围将取决于组织获取足够信息的能力、获取信息的成本以及该关系可能带来的贿赂风险程度等因素。

c) 组织对其商业合作伙伴实施的尽职调查程序应在类似贿赂风险水平上保持一致（例如，在高贿赂风险地点或市场中，高贿赂风险的商业合作伙伴可能需要比低贿赂风险地点或市场中的低贿赂风险商业合作伙伴进行更高水平的尽职调查）。

d) 不同类型的商业合作伙伴可能需要不同水平的尽职调查，例如：

1) 从组织潜在的法律和财务责任角度来看，当商业合作伙伴代表组织行事或为组织谋利时，它们对组织构成的贿赂风险高于仅向组织提供产品或服务时。例如，协助组织获得合同授予的代理人可能向组织客户的经理行贿以帮助组织赢得合同，因此组织可能对代理人的腐败行为负责。因此，组织对代理人的尽职调查可能尽可能全面。另一方面，向组织出售设备或材料的供方，如果与组织的客户或与组织活动相关的公职人员没有涉及，则不太可能代表组织或为组织谋利而行贿，因此对供方的尽职调查水平可以较低。

2) 组织对其商业合作伙伴的影响力也影响组织作为尽职调查的一部分直接从这些商业合作伙伴获取信息的能力。组织可能相对容易要求其代理人和合资伙伴在组织承诺与他们合作之前提供关于他们自己的广泛信息，因为在这种情况下，组织对与谁签订合同有一定程度的选择权。然而，组织可能更难要求客户或客户提供关于他们自己的信息或填写尽职调查问卷。这可能是由于组织对客户或客户没有足够的影响力来这样做（例如，当组织参与竞争性投标以向客户提供服务时）。

e) 组织对其商业合作伙伴进行的尽职调查可能包括，例如：

1) 向商业合作伙伴发送问卷，要求其回答 A. 10. 3. a) 中提到的问题。

2) 在网络上搜索商业合作伙伴及其股东和高层管理的信息，以识别任何与贿赂相关的信息。

3) 搜索适当的政府、司法和国际资源以获取相关信息。

4) 检查国家或地方政府或多边机构（如世界银行）保持的公开可用的被限制或禁止与公共或政府实体签订合同的组织名单。

5) 向其他适当方询问商业合作伙伴的道德声誉。

6) 任命具有相关专业知识的其他人或组织协助尽职调查过程。

f) 可以根据初步尽职调查的结果向商业合作伙伴提出进一步的问题（例如，解释任何不利信息）。

A. 10.4 尽职调查的局限性

尽职调查并非完美工具。没有负面信息并不一定意味着商业合作伙伴不构成贿赂风险。负面信息也并不一定意味着商业合作伙伴构成贿赂风险。然而，组织需要仔细评估结果，并根据其掌握的事实做出理性判断。总体意图是，组织应对商业合作伙伴进行合理且相称的调查，考虑到商业合作伙伴将开展的活动以及这些活动固有的贿赂风险，以便对组织与该商业合作伙伴合作时所面临的贿赂风险水平做出合理判断。

A. 10.5 人员尽职调查包含在A. 8中。

A. 11 财务控制

财务控制是组织为妥善管理其财务交易，并准确、完整、及时地记录这些交易所实施的管理体系和过程。设计良好的反贿赂财务控制机制作为制衡手段，通过提高被发现的风险并收集信息以支持调查，从而遏制不当行为。根据组织的规模和交易情况，组织实施的能够降低贿赂风险的财务控制措施可以包括，例如：

- a) 实施职责分离，确保同一人不能同时发起和批准付款；
- b) 实施适当的分级审批权限，以便较大交易需要更高级别管理层的批准；
- c) 核实收款人的任命以及所执行的工作或服务已经得到组织相关审批机制的批准；
- d) 要求付款审批至少需有两个签名；
- e) 要求将适当的支持性文件附在付款审批单上；
- f) 限制现金使用，并实施有效的现金控制方法；
- g) 要求账户中的付款分类和描述准确清晰；
- h) 按策划的时间间隔对重大财务交易进行管理评审；
- i) 按策划的时间间隔实施独立财务审计，并同样按计划间隔更换执行审计的个人或组织。

A. 12 非财务控制

非财务控制是组织实施的管理体系和过程，以帮助其确保采购、运营、商业及其他非财务方面的活动得到妥善管理。根据组织和交易的规模，组织为降低贿赂风险而实施的采购、运营、商业及其他非财务控制可包括以下控制措施，例如：

- a) 使用经过预审合格过程的批准承包商、分包商、供方和咨询顾问，在该过程中评估其参与贿赂的可能性；此过程可能包括 A. 10 条款中规定的尽职调查类型；
- b) 评估：
 - 1) 商业伙伴（不包括客户或客户）向组织提供的服务的必要性和合法性；
 - 2) 服务是否得到妥善执行；

3) 向商业伙伴支付的任何款项相对于这些服务是否合理且相称。这一点特别重要，以避免商业伙伴利用组织支付给其的部分款项代表组织或为了组织的利益而行贿的风险。例如，如果组织任命了一名代理人协助销售，并在组织获得合同时向其支付佣金或有费用，组织需要合理确信佣金支付相对于代理人实际提供的合法服务是合理且相称的，同时考虑到若合同未授予时代理人承担的风险。如果支付的佣金或有费用过高，则代理人利用其中部分款项诱使公职人员或组织客户的雇员将合同授予组织的风险就会增加。组织还可要求其商业伙伴提供文件证明服务已提供：

c) 在可能和合理的情况下，仅在至少三个竞争者之间经过公平且适当时透明的竞争性招标过程后，才授予合同；

d) 要求至少两人评估投标并批准合同的授予；

e) 实施职责分离，使批准合同签订的人员与请求合同签订的人员不同，且来自与管理合同或批准合同项下所完成工作的人员不同的部门或职能；

f) 要求至少两人在合同上以及更改合同条款或批准合同项下所开展工作或提供供应的文件上签字；

g) 对潜在高贿赂风险的交易实施更高层次的管理监督；

h) 通过限制适当人员的访问，保护投标和其他价格敏感信息的完整性；

i) 提供适当的工具和模板以协助人员（例如实用指南、应做和不应做的事项、审批阶梯、检查表、表格、IT 工作流程）。

注：ISO 37301 中给出了更多控制示例和指导。

A.13 受控组织和商业伙伴反贿赂管理体系的实施

A.13.1 总则

A.13.1.1 8.5条要求的原因是，受控组织和商业伙伴都可能给组织带来贿赂风险。组织在这些情况下旨在避免的贿赂风险类型包括，例如：

a) 组织的子公司行贿，导致组织可能承担责任；

b) 合资企业或合资伙伴行贿以赢得组织参与的合资企业的工作；

c) 客户或客户的采购经理要求组织行贿以换取合同授予；

d) 在客户或公职人员可能从任命中个人受益的情况下，组织的客户要求组织任命特定的分包商或供方；

e) 组织的代理人代表组织向组织客户的经理行贿；

f) 组织的供方或分包商向组织的采购经理行贿以换取合同授予。

A. 13. 1. 2 如果受控组织或商业伙伴已针对这些风险实施了反贿赂控制，则组织面临的贿赂风险通常会降低。

A. 13. 1. 3 8.5条的要求区分了组织能够控制的组织和无法控制的组织。就本要求而言，如果组织直接或间接控制另一组织的管理，则视为对该组织具有控制权。例如，组织可以通过董事会多数投票或通过多数持股对子公司、合资企业或联合体拥有控制权。仅仅因为组织与另一组织有大量业务往来，并不意味着就本要求而言，组织对该另一组织拥有控制权。

A. 13. 2 受控组织

A. 13. 2. 1 有理由期望组织要求其控制的任何其他组织实施合理且相称的反贿赂控制。这可以通过受控组织实施与组织自身相同的反贿赂管理体系，或者由受控组织实施其自己的特定反贿赂控制来实现。这些控制应考虑根据4.5进行的贿赂风险评估，针对受控组织面临的贿赂风险而言，应是合理且相称的。

A. 13. 2. 2 当商业伙伴由组织控制时（例如，组织对其具有管理控制权的合资企业），该受控商业伙伴应遵守8.5.1中的要求。

A. 13. 3 非受控商业伙伴

A. 13. 3. 1 对于组织不控制的商业伙伴，在以下情况下，组织可能不需要采取8.5.2所要求的步骤来要求商业伙伴实施反贿赂控制：

a) 商业伙伴不存在或存在较低的贿赂风险；或

b) 商业伙伴存在的贿赂风险超过低风险，但商业伙伴可以实施的控制措施无助于缓解相关风险（坚持要求商业伙伴实施无助于缓解风险的控制措施毫无意义；然而，在这种情况下，组织应在其风险评估中考虑这一因素，以指导关于如何以及是否继续与该商业伙伴合作的决策）。

A. 13. 3. 2 这反映了本标准的合理性和相称性。

A. 13. 3. 3 如果贿赂风险评估（见4.5）或尽职调查（见8.2）得出结论，认为非受控商业伙伴存在超过低风险的贿赂风险，且商业伙伴实施的反贿赂控制有助于缓解这种贿赂风险，组织应在8.5下采取以下进一步步骤：

a) 组织确定商业伙伴是否已实施适当的反贿赂控制来管理相关贿赂风险。组织应在进行适当的尽职调查后（见条款A.10）做出这一确定。组织试图验证这些控制是否管理了与组织和商业伙伴之间交易相关的贿赂风险。组织无需验证商业伙伴是否对其更广泛的贿赂风险有控制措施。请注意，控制的范围和组织需要采取的验证这些控制的步骤都应与其相关贿赂风险合理且相称。如果组织已尽其合理能力确定商业伙伴已实施适当的控制，则就该商业伙伴而言，已满足8.5的要求。

b) 如果组织发现商业伙伴没有实施适当的反贿赂控制来管理相关贿赂风险，或者无法验证其是否已实施这些控制，组织应采取以下进一步步骤：

1) 如果可行，组织要求商业伙伴就相关交易、项目或活动实施反贿赂控制；

2) 如果要求商业伙伴实施反贿赂控制不可行，组织在评估商业伙伴带来的贿赂风险以及组织管理这些风险的方式时，应考虑这一因素。这并不意味着组织不能继续与该商业伙伴建立关系或进行交易。然而，作为贿赂风险评估的一部分，组织应考虑商业伙伴涉及贿赂的可能性，并在评估整体贿赂风险时考虑缺乏此类控制的因素。如果组织认为该商业伙伴带来的贿赂风险不可接受地高，且无法通过其他方式（例如重新构建交易）降低贿赂风险，则适用 8.8 条的规定。

A. 13.3.4 组织是否要求非受控商业伙伴实施控制，取决于具体情况。例如：

a) 当组织对商业伙伴具有相当程度的影响力时，通常要求是可行的。例如，当组织任命某代理代表其进行交易，或任命工作范围较大的分包商时。在此情况下，组织通常能够将实施反贿赂控制作为任命的条件；

b) 当组织对商业伙伴不具有相当程度的影响力时，通常要求不可行，例如：

1) 项目的客户；

2) 客户指定的特定分包商或供方；

3) 主要分包商或供方，当其议价能力远大于组织时（例如，当组织按供方的标准条款从主要供方处购买组件时）。

c) 当商业伙伴缺乏实施控制所需的资源或专业知识时，通常要求不可行。

A. 13.3.5 A. 13.3.5 组织所要求的控制类型取决于具体情况。这些控制应合理且与贿赂风险相称，并至少应在其范围内包含相关的贿赂风险。根据商业伙伴的性质及其所带来的贿赂风险性质，组织可采取以下步骤，例如：

a) 对于工作范围大且复杂、贿赂风险高的商业伙伴，组织可要求其实施与本标准要求相当的控制，以应对其给组织带来的贿赂风险。

b) 对于中等规模和中等贿赂风险的商业伙伴，组织可要求其就交易实施一些最低限度的反贿赂要求，例如：反贿赂方针、对相关员工的培训、负责交易合规的管理人员、对关键支付的控制以及报告渠道。

c) 对于工作范围非常具体的小型商业伙伴（例如代理或小供方），组织可要求对相关员工进行培训，并对关键支付、礼品和招待进行控制。

A. 13.3.6 这些控制仅需在组织与商业伙伴之间的交易中实施（尽管在实践中，商业伙伴可能对其整个业务都实施了控制）。

A. 13.3.7 以上仅为示例。重要的是，组织应识别交易中的关键贿赂风险，并尽可能要求商业伙伴对这些关键贿赂风险实施合理且相称的控制。

A. 13.3.8 组织通常会将这些要求作为与非受控商业伙伴合作的前提条件和/或作为合同文件的一部分。

A. 13.3.9 组织无需验证非受控商业伙伴是否完全遵守这些要求。然而，组织应采取合理步骤，确信商业伙伴正在遵守（例如，要求商业伙伴提供其相关政策文件的副本）。在高贿赂风险情况下（例如代理），组织可实施监视、报告和/或审计程序。

A. 13.3.10 由于实施反贿赂控制可能需要一些时间，因此组织给予其商业伙伴时间实施这些控制可能是合理的。在此期间，组织可继续与该商业伙伴合作，但缺乏这些控制将是风险评估和尽职调查中的一个考虑因素。然而，如果商业伙伴未能及时有效地实施所要求的控制，组织应考虑要求享有终止相关合同或协议的权利。

A. 14 反贿赂承诺

A. 14.1 获取反贿赂承诺的要求仅适用于那些存在高于低风险贿赂风险的商业伙伴。

A. 14.2 交易中的贿赂风险可能较低的情况包括，例如：

- a) 当组织购买少量极低价值物品时；
- b) 当组织直接从航空公司或酒店在线预订机票或酒店房间时；
- c) 当组织直接向客户提供低价值商品或服务时（如食品、电影票）。

A. 14.3 在这些情况下，组织无需从这些低贿赂风险的供方或客户那里获取反贿赂承诺。

A. 14.4 对于存在高于低风险贿赂风险的商业伙伴，组织应在可行的情况下，从该商业伙伴那里获取反贿赂承诺。

a) 当组织对商业伙伴有影响力，并能坚持要求商业伙伴作出这些承诺时，通常要求这些承诺是可行的。例如，当组织任命代理代表其在交易中行事，或任命工作范围广泛的分包商时，组织很可能能够要求这些承诺；

b) 组织可能没有足够的影响力来要求这些承诺，例如，在与主要客户或客户的交易中，或当组织按照供方的标准条款从主要供方处购买组件时。在这些情况下，缺乏此类条款并不意味着项目或关系不应继续进行，但缺乏此类承诺应被视为贿赂风险评估和根据 4.5 和 8.2 进行的尽职调查中的一个相关因素。

A. 14.5 这些承诺应尽可能以书面形式获得。这可以作为一份单独的承诺文件，也可以作为组织与商业伙伴之间合同的一部分。

A. 15 礼品、招待、捐赠及类似好处

A. 15.1 组织需要意识到，礼品、招待、捐赠及其他好处可能被第三方（如商业竞争对手、媒体、检察官或法官）视为贿赂目的，即使给予者和接受者均无此意图。一个有用的控制机制是尽可能避免任何可能被第三方合理视为贿赂目的的礼品、招待、捐赠及其他好处。

A. 15.2 8.7中提及的好处可包括，例如：

- a) 礼品、娱乐和招待；
- b) 政治或慈善捐赠；
- c) 客户代表或公职人员旅行；
- d) 宣传费用；
- e) 赞助；
- f) 社区好处；
- g) 培训；
- h) 俱乐部会员资格；
- i) 个人恩惠；
- j) 机密和特权信息。

A. 15.3 关于礼品和招待，组织实施的程序可例如设计为：

- a) 通过以下方式控制礼品和招待的程度和频率：
 - 1) 全面禁止所有礼品和招待；
 - 2) 允许礼品和招待，但根据以下因素加以限制：
 - 最大支出（可根据地点和礼品及招待的类型而有所不同）；
 - 频率（相对较小的礼品和招待如果重复发生，可能累积成较大金额）；
 - 时间（例如，不在招标谈判期间或紧接其前后）；
 - 合理性（考虑地点、行业和给予者或接受者的职位）；
 - 接受者身份（例如，那些有权授予合同或批准许可、证书或付款的人）；
 - 互惠性（组织内任何人不得接受价值超过其被允许给予的礼品或招待）；
 - 法律和监管环境（某些地点和组织可能有禁止或控制措施）；
- b) 要求超过规定价值或频率的礼品和招待需事先获得适当管理人员的批准；
- c) 要求超过规定价值或频率的礼品和招待需公开进行，有效记录（例如，在登记册或会计账簿中），并受到监督。

A. 15.4 关于政治或慈善捐赠、赞助、宣传费用和社区好处，组织实施的程序可例如设计为：

- a) 禁止旨在影响或可能被合理认为影响招标或其他有利于组织的决定的支付；
- b) 对政治党派、慈善机构或其他接受者进行尽职调查，以确定其是否合法且未被用作贿赂渠道（例如，在互联网上搜索或进行其他适当查询，以确认政治党派或慈善机构的管理人员是否有贿赂或类似犯罪行为的声誉，或与组织的项目或客户有关联）；

-
- c) 要求适当管理人员批准支付；
 - d) 要求公开披露支付；
 - e) 确保支付符合适用法律和法规的规定；
 - f) 避免在合同谈判之前、期间或紧接其后进行捐赠。

A. 15.5 关于客户代表或公职人员旅行，组织实施的程序可例如设计为：

- a) 仅允许符合客户或公共机构程序以及适用法律和法规的支付；
- b) 仅允许对客户代表或公职人员正确履行职责所必要的旅行（例如，检查组织工厂的质量程序）；
- c) 要求组织内的适当管理人员批准支付；
- d) 如可能，要求通知公职人员的上级或雇主或反贿赂职能部门所提供的旅行和招待；
- e) 将支付限制在与合理旅行行程直接相关的必要旅行、住宿和餐饮费用；
- f) 根据组织的礼品和招待政策，将相关娱乐限制在合理水平；
- g) 禁止支付家庭成员或朋友的费用；
- h) 禁止支付假期或娱乐费用。

A. 16 内部审核

A. 16.1 9.2的要求并不意味着组织必须拥有自己的独立内部审核部门。它要求组织任命一个合适、有能力和独立的部门或个人，负责进行此审核。组织可以委托第三方来运营其整个内部审核计划，或者聘请第三方来执行现有计划中的某些部分。

A. 16.2 审核的频率取决于组织的需求。很可能每年都会选择一些样本项目、合同、程序、控制和系统进行审核。

A. 16.3 样本的选择可以基于风险，例如，高风险贿赂项目将优先于低风险贿赂项目被选中进行审核。

A. 16.4 审核通常需要提前计划，以便相关方准备好必要的文件和时间。然而，在某些情况下，组织可能会发现实施一次被审核方未预期的审核是有用的。

A. 16.5 如果组织设有管理机构，管理机构也可以根据其认为必要的情况，指导组织选择审核项目和审核频率，以行使独立性并帮助确保审核针对组织的主要贿赂风险领域。管理机构还可能要求获取所有审核报告和结果，并要求在审核完成后，将任何识别出特定类型较高贿赂风险问题或贿赂风险指标的审核情况报告给管理机构。

A. 16.6 审核的目的是为管理机构 and 高层管理提供合理保证，证明反贿赂管理体系已得到实施并有效运行，以助于预防和发现贿赂行为，并对任何可能腐败的人员形成威慑（因为他们会意识到他们的项目或部门可能会被选中进行审核）。

A.17 成文信息

7.5.1中的成文信息可能包括：

- a) 人员接收反贿赂方针的确认；
- b) 向存在高于低风险贿赂风险的商业伙伴提供反贿赂方针；
- c) 反贿赂管理体系的政策、程序和控制措施；
- d) 贿赂风险评估结果（见 4.5）；
- e) 提供的反贿赂培训（见 7.3）；
- f) 进行的尽职调查（见 8.2）；
- g) 为实施反贿赂管理体系所采取的措施；
- h) 赠送和接受的礼品、招待、捐赠和类似利益的审批和记录（见 8.7）；
- i) 与以下方面相关的担忧所采取的行动及结果：
 - 1) 反贿赂管理体系的任何弱点；
 - 2) 试图、涉嫌或实际的贿赂事件；
- j) 组织或第三方进行的监视、调查或审核的结果。

A.18 调查和处理贿赂问题

A.18.1 本标准要求组织就如何调查和处理任何报告、发现或有合理理由怀疑的贿赂问题或违反反贿赂控制措施的行为，实施适当的程序。组织如何调查和处理特定问题将取决于具体情况。每种情况都不同，组织的应对措施应合理且与情况相称。对于涉嫌贿赂的重大问题报告，需要采取比违反反贿赂控制措施的轻微行为更为紧急、重大和详细的行动。以下建议仅供指导，不应视为规定性要求。

A.18.2 反贿赂职能部门最好是任何涉嫌或实际贿赂行为或违反反贿赂控制措施行为的报告的接收者。如果报告首先提交给其他人，组织的程序应要求尽快将报告转交给反贿赂职能部门。在某些情况下，反贿赂职能部门本身会发现嫌疑或违规行为。

A.18.3 程序应确定谁有责任决定如何调查和处理该问题。例如：

- a) 小型组织可实施一项程序，根据该程序，所有问题，无论大小，均应由反贿赂职能部门立即报告给最高管理者，由最高管理者决定如何应对；
- b) 大型组织可实施一项程序，根据该程序：
 - 轻微问题由反贿赂职能部门处理，并按计划间隔向最高管理者提交所有轻微问题的总结报告；
 - 重大问题由反贿赂职能部门立即报告给最高管理者，由最高管理者决定如何应对。

A. 18.4 当发现任何问题时，最高管理者或反贿赂职能部门（视情况而定）应评估已知事实和问题的潜在严重性。如果他们尚未掌握足够的事实来做出决定，则应开始调查。

A. 18.5 调查应由未涉及该问题的人员进行。可以是反贿赂职能部门、内部审计部门、其他适当的管理人员或适当的第三方。最高管理者应给予调查人员适当的权力、资源和访问权限，以便有效进行调查。调查人员最好应接受过调查方面的培训或具有先前经验。调查应及时查明事实，并通过以下方式收集所有必要证据：

- a) 进行询问以查明事实；
- b) 收集所有相关文件和其他证据；
- c) 获取证人证据；
- d) 在可能且合理的情况下，要求就问题作出书面报告，并由报告人签字。

A. 18.6 在进行调查和任何后续行动时，组织需要考虑相关因素，例如：

- a) 适用的法律（可能需要法律咨询）；
- b) 人员的安全；
- c) 发表声明时的诽谤风险；
- d) 保护报告人员以及报告中涉及或提及的其他人员（见 8.9）；
- e) 对组织和个人的潜在刑事、民事和行政责任、经济损失和声誉损害；
- f) 向当局报告的法律义务或对组织有利的因素；
- g) 在事实查明之前，对问题和调查保密；
- h) 最高管理者需要要求人员在调查中予以充分配合。

A. 18.7 调查结果应适当报告给最高管理者或反贿赂职能部门。如果结果报告给最高管理者，也应通报给反贿赂职能部门。

A. 18.8 一旦组织完成调查，和/或掌握足够信息能够做出决定，组织应采取适当的后续行动。根据具体情况和问题的严重性，这些行动可以包括以下一项或多项：

- a) 终止、退出或修改组织在项目、交易或合同中的参与；
- b) 偿还或追回获得的任何不当利益；
- c) 对负责人员进行纪律处分（根据问题的严重性，可以从对轻微违规行为的警告到对严重违规行为的解雇）；
- d) 向当局报告该事项；

e) 如果发生贿赂，采取行动避免或处理任何可能的后续法律违法行为（例如，在账户中虚假描述贿赂可能发生的虚假会计，贿赂被错误地从收入中扣除时可能发生的税务违法行为，或处理犯罪所得时可能发生的洗钱行为）。

A. 18.9 组织应评审其反贿赂程序，以检查问题是否由于其程序中的某些不足而产生，如果是，应立即采取适当步骤改进其程序。

A. 19 监视

A. 19.1 反贿赂管理体系的监视可能包括但不限于以下方面：

- a) 培训的有效性；
- b) 控制措施的有效性，例如通过抽样测试输出结果来验证；
- c) 为满足反贿赂管理体系要求所分配职责的有效性；
- d) 对之前已识别的合规失败情况的处理有效性；
- e) 未按计划执行内部审计的情况。

A. 19.2 合规绩效的监视可能包括但不限于以下方面：

- 不合规情况和“未遂事件”（即未造成不良影响的事件）；
- 未满足反贿赂要求的情况；
- 未达成目标的情况；
- 合规文化的现状。

注：参见ISO 37301。

A. 19.3 组织可以按策划的时间间隔，在整个组织或组织的部分部门进行自我评估，以评估反贿赂管理体系的有效性（见9.4）。

A. 20 策划和实施变更

A. 20.1 应通过多种方法（如内部审计（见9.2）、管理层评审（见9.3）和反贿赂职能评审（见9.4））持续且定期地评估反贿赂管理体系的充分性和有效性。

A. 20.2 组织应考虑这些评估的结果和输出，以确定是否有必要或有机会对反贿赂管理体系进行变更。

A. 20.3 为了帮助确保反贿赂管理体系的完整性和有效性得以保持，对管理体系中单个要素的变更应考虑这种变更对管理体系整体有效性的依赖性和影响。

A. 20.4 当组织确定需要对反贿赂管理体系进行变更时，这些变更应以计划的方式进行，并考虑以下因素：

- a) 变更的目的及其潜在后果；

-
- b) 反贿赂管理体系的完整性；
 - c) 资源的可获得性；
 - d) 职责和权限的分配或重新分配；
 - e) 变更的实施速率、程度和时间框架。

A. 20.5 因应对任何不符合项（见10.2）而采取的措施以及因持续改进（见10.1）而对反贿赂管理体系进行的增强，应按照相同的方法进行。

A. 21 公职人员

A. 21.1 在许多反腐败法律中，“公职人员”（见3.26）一词的定义较为宽泛。

A. 21.2 以下列表并非穷尽，且并非所有示例都适用于所有司法管辖区。在评估贿赂风险时，组织应考虑其与之打交道或可能打交道的公职人员类别。

A. 21.3 公职人员一词可能包括以下人员：

- a) 国家、州/省或市级公职人员，包括立法机构成员、行政公职人员和司法人员；
- b) 政党官员；
- c) 公职候选人；
- d) 政府雇员，包括各部委、政府机构、行政法庭和公共委员会的雇员；
- e) 国际公共组织的官员，如世界银行、联合国、国际货币基金组织的官员；
- f) 国有企业雇员，除非该企业在相关市场上以正常的商业基础运营，即基本上相当于私营企业的运营基础，没有优惠补贴或其他特权（见参考文献[19]）。

A. 21.4 在许多司法管辖区，公职人员的亲属和密切关联人员也被视为反腐败法律意义上的公职人员。

A. 22 反贿赂倡议

虽然本标准并未要求，但组织可能会发现参与或考虑任何行业或其他反贿赂倡议的建议是有益的，这些倡议旨在推广或发布与组织活动相关的良好反贿赂实践。

参 考 文 献

- [1] ISO 9000, 《质量管理体系—基础和术语》
- [2] ISO 9001, 《质量管理体系—要求》
- [3] ISO 14001, 《环境管理体系—使用指南的要求》
- [4] ISO/IEC 17000, 《合格评定—词汇和通用原则》
- [5] ISO 19011, 《管理体系审核指南》
- [6] ISO 22000, 《食品安全管理体系—食品链中各类组织的要求》
- [7] ISO 26000, 《社会责任指南》
- [8] ISO/IEC 27001, 《信息安全、网络安全与隐私保护—信息安全管理体系—要求》
- [9] ISO 31000, 《风险管理—指南》
- [10] ISO 31022, 《风险管理—法律风险管理指南》
- [11] ISO 37000:2021, 《组织治理—指南》
- [12] ISO 37002, 《举报管理体系—指南》
- [13] ISO/TS 37008, 《组织内部调查—指南》
- [14] ISO 37009, 《组织利益冲突—指南》
- [15] ISO 37301, 《合规管理体系—使用指南的要求》
- [16] ISO/IEC 导则2, 《标准化及相关活动—通用词汇》
- [17] 《联合国反腐败公约》, 纽约, 2004年, 详见:

https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

- [18] 经济合作与发展组织, 《打击国际商业交易中贿赂外国公职人员公约及相关文件》, 巴黎, 2010年
- [19] 经济合作与发展组织, 《内部控制、道德与合规良好实践指南》, 巴黎, 2010年
- [20] 经济合作与发展组织, 《关于打击国际商业交易中贿赂外国公职人员公约的评注》, 1997年11月21日
- [21] 联合国全球契约/透明国际, 《反腐败第十项原则报告指南》, 2009年

-
- [22] 国际商会、透明国际、联合国全球契约及世界经济论坛，《RESIST：抵制国际交易中的勒索和索贿—企业员工培训工具》，2010年
- [23] 国际商会，《反腐败规则》，巴黎，2011年
- [24] 透明国际，《反贿赂商业原则及配套工具》，柏林，2013年
- [25] 透明国际，《腐败感知指数》
- [26] 透明国际，《行贿者指数》
- [27] 世界银行，《全球治理指标》
- [28] 国际公司治理网络，《ICGN反腐败实践声明与指南》，伦敦，2009年
- [29] 世界经济论坛，合作伙伴