SLOVENSKI STANDARD
SIST ISO 37001:2016

01-december-2016

Sistemi vodenja za preprečevanje korupcije - Zahteve z navodili za uporabo

Anti-bribery management systems - Requirements with guidance for use

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

Ta slovenski standard je istoveten z: **ISO 37001:2016**

ICS:

03.100.02	Upravljanje in etika	Governance and ethics
03.100.70	Sistemi vodenja	Management systems

SIST ISO 37001:2016 **en,fr**

INTERNATIONAL STANDARD

ISO 37001

First edition
2016-10-15

Anti-bribery management systems — Requirements with guidance for use

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

Reference number
ISO 37001:2016(E)

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

Contents

Page

Foreword

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

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

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

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

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

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

Introduction

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

Governments have made progress in addressing bribery through international agreements such as the Organization for Economic Co-operation and Development Convention on Combating Bribery of Foreign Public Officials in International Business Transactions[15] and the United Nations Convention against Corruption[14] and through their national laws. In most jurisdictions, it is an offence for individuals to engage in bribery and there is a growing trend to make organizations, as well as individuals, liable for bribery.

However, the law alone is not sufficient to solve this problem. Organizations have a responsibility to proactively contribute to combating bribery. This can be achieved by an anti-bribery management system, which this document is intended to provide, and through leadership commitment to establishing a culture of integrity, transparency, openness and compliance. The nature of an organization's culture is critical to the success or failure of an anti-bribery management system.

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

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

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

In this document, the following verbal forms are used:

— "shall" indicates a requirement;

— "should" indicates a recommendation;

— "may" indicates a permission;

— "can" indicates a possibility or a capability.

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

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

Anti-bribery management systems — Requirements with guidance for use

1 Scope

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

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

— bribery by the organization;

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

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

— bribery of the organization;

— bribery of the organization's personnel in relation to the organization's activities;

— bribery of the organization's business associates in relation to the organization's activities;

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

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

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

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

NOTE 1 See Clause A.2 for guidance.

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

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
bribery
offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the *performance* (3.16) of that person's duties

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

3.2
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.11)

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

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

3.3
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.2) that can affect, be affected by, or perceive itself to be affected by a decision or activity

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

3.4
requirement
need that is stated and obligatory

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 and interested parties that the need or expectation under consideration is implied.

Note 3 to entry: A specified requirement is one that is stated, for example in documented information.

3.5
management system
set of interrelated or interacting elements of an *organization* (3.2) to establish *policies* (3.10) and *objectives* (3.11) and *processes* (3.15) to achieve those objectives

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.

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

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

3.7
governing body
group or body that has the ultimate responsibility and authority for an *organization's* (3.2) activities, governance and policies and to which *top management* (3.6) reports and by which top management is held accountable

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

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

3.8
anti-bribery compliance function
person(s) with responsibility and authority for the operation of the anti-bribery *management system* (3.5)

3.9
effectiveness
extent to which planned activities are realized and planned results achieved

3.10
policy
intentions and direction of an *organization* (3.2), as formally expressed by its *top management* (3.6) or its *governing body* (3.7)

3.11
objective
result to be achieved

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

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

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

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

3.12
risk
effect of uncertainty on *objectives* (3.11)

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

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

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

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

3.13
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 which transforms inputs into outputs

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 the management of activities, *processes* (3.15), products (including services), systems or *organizations* (3.2).

3.17
outsource (verb)
make an arrangement where an external *organization* (3.2) performs part of an organization's function or *process* (3.14)

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

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

3.18
monitoring
determining the status of a system, a *process* (3.15) or an activity

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

3.19
measurement
process (3.15) to determine a value

3.20
audit
systematic, independent and documented *process* (3.15) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

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

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

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

3.21
conformity
fulfilment of a *requirement* (3.4)

3.22
nonconformity
non-fulfilment of a *requirement* (3.4)

3.23
corrective action
action to eliminate the cause of a *nonconformity* (3.22) and to prevent recurrence

3.24
continual improvement
recurring activity to enhance *performance* (3.16)

3.25
personnel
organization's (3.2) directors, officers, employees, temporary staff or workers, and volunteers

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

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

3.26
business associate
external party with whom the *organization* (3.2) has, or plans to establish, some form of business relationship

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

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

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

3.27
public official
person holding a legislative, administrative or judicial office, whether by appointment, election or succession, or any person exercising a public function, including for a public agency or public enterprise, or any official or agent of a public domestic or international organization, or any candidate for public office

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

3.28
third party
person or body that is independent of the *organization* (3.2)

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

3.29
conflict of interest
situation where business, financial, family, political or personal interests could interfere with the judgment of persons in carrying out their duties for the *organization* (3.2)

3.30
due diligence
process (3.15) to further assess the nature and extent of the bribery *risk* (3.12) and help *organizations* (3.2) make decisions in relation to specific transactions, projects, activities, *business associates* (3.26) and personnel

4 Context of the organization

4.1 Understanding the organization and its context

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

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

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

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

d) the organization's business model;

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

f) the organization's business associates;

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

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

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

4.2 Understanding the needs and expectations of stakeholders

The organization shall determine:

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

b) the relevant requirements of these stakeholders.

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

4.3 Determining the scope of the anti-bribery management system

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

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2;

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

The scope shall be available as documented information.

NOTE See Clause A.2 for guidance.

4.4 Anti-bribery management system

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

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

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

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

NOTE 2 See Clause A.3 for guidance.

4.5 Bribery risk assessment

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

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

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

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

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

4.5.3 The bribery risk assessment shall be reviewed:

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

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

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

NOTE See Clause A.4 for guidance.