DRAFT INTERNATIONAL STANDARD

ISO/DIS 37002

ISO/TC **309** Secretariat: **BSI**

Voting begins on:
2020-06-08

Voting terminates on:
2020-08-31

Whistleblowing management systems — Guidelines

ICS: 03.100.02; 03.100.01; 03.100.70

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 37002:2020(E)

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

Published in Switzerland

Contents

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 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*.

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

Whistleblowing is the act of reporting suspected wrongdoing, or risk of wrongdoing. Studies and experience demonstrate that a large proportion of wrongdoing comes to the attention of the affected organization via reports from persons within or close to the organization.

Organizations are increasingly introducing internal whistleblowing policies and processes in response to regulation or on a voluntary basis.

This document provides guidance to organizations for establishing, implementing, maintaining and improving a whistleblowing management system, with the following outcomes:

a) encouraging and facilitating reporting of wrongdoing;

b) supporting and protecting whistleblowers and other persons involved;

c) ensuring reports of wrongdoing are dealt with in a proper and timely manner;

d) improving organizational culture, governance and the prevention of wrongdoing.

Potential benefits for the organization include:

— allowing the organization to identify and address wrongdoing at the earliest opportunity;

— helping prevent or minimize loss of assets and aiding recovery of lost assets;

— ensuring compliance with organizational policies, procedures, and legal and social obligations;

— attracting and retaining personnel committed to the organization's values and culture; and

— demonstrating sound, ethical governance practices to society, markets, regulators, owners and other stakeholders.

An effective whistleblowing management system will build organizational trust, by:

— demonstrating leadership commitment to preventing and addressing wrongdoing;

— encouraging people to come forward early with reports of wrongdoing;

— reducing and preventing detrimental treatment of whistleblowers and others involved; and

— encouraging a culture of openness, transparency and accountability.

This document provides guidance for organizations to create a whistleblowing management system based on principles of trust, impartiality and protection. It is adaptable, and its use will vary with the size, nature, complexity and jurisdiction of the organization's activities. It may assist an organization to improve its existing whistleblowing policy and procedures, or to comply with applicable whistleblowing legislation.

This document adopts the "high-level structure" (i.e. clause sequence, common text and common terminology) developed by ISO to improve alignment among International Standards for management systems. Organizations may adopt this document as stand-alone guidance for their organization or along with other management system standards, including to address whistleblowing-related requirements in other management systems.

Figure 1 is a conceptual overview of a recommended whistleblower management system showing how the concepts of 'Trust', 'Impartiality' and 'Protection' overlay all elements of such a system.

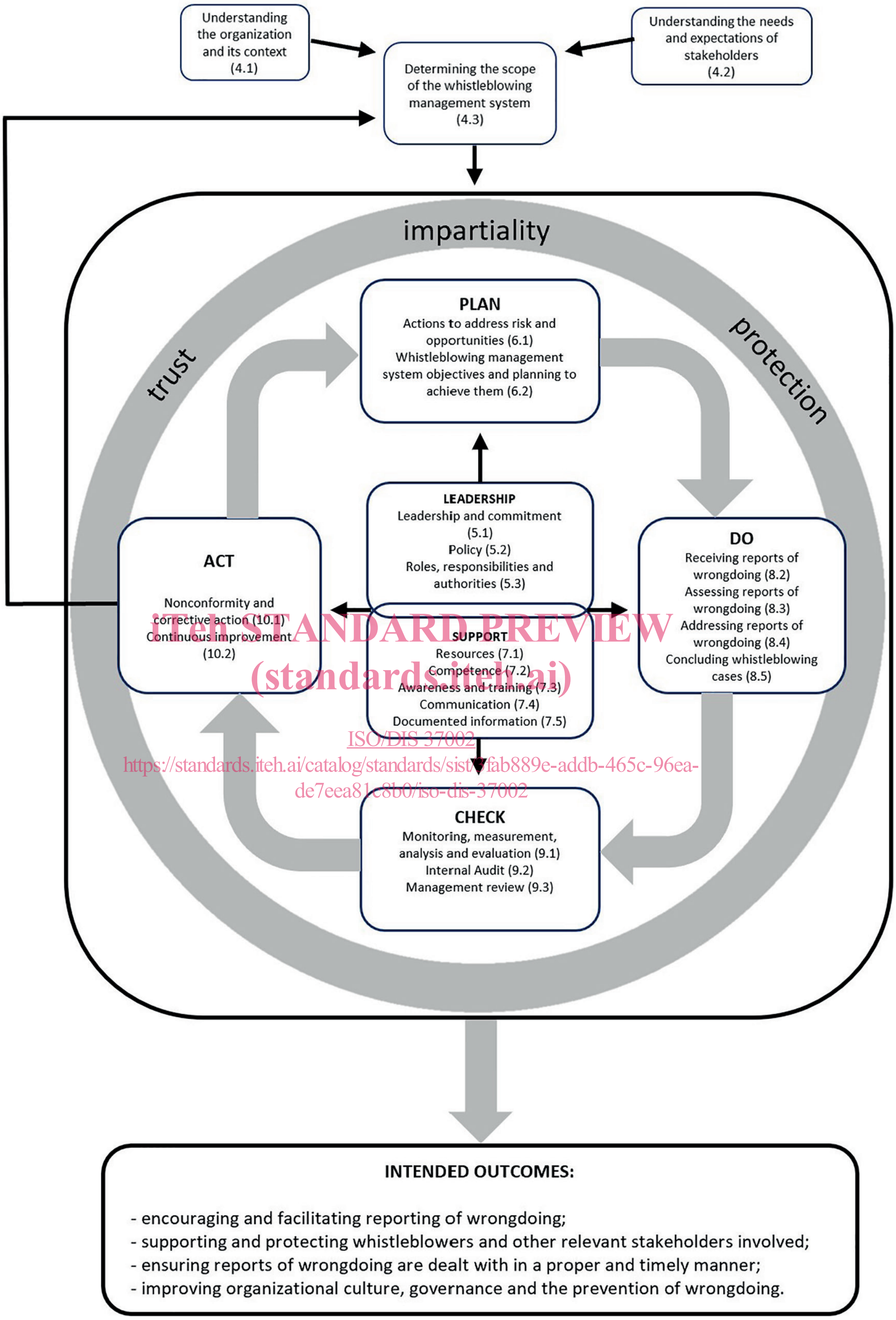
Understanding the organization and its context (4.1)
Determining the scope of the whistleblowing management system (4.3)
Understanding the needs and expectations of stakeholders (4.2)
impartiality
trust
protection
PLAN
Actions to address risk and opportunities (6.1)
Whistleblowing management system objectives and planning to achieve them (6.2)
LEADERSHIP
Leadership and commitment (5.1)
Policy (5.2)
Roles, responsibilities and authorities (5.3)
ACT
Nonconformity and corrective action (10.1)
Continuous improvement (10.2)
DO
Receiving reports of wrongdoing (8.2)
Assessing reports of wrongdoing (8.3)
Addressing reports of wrongdoing (8.4)
Concluding whistleblowing cases (8.5)
SUPPORT
Resources (7.1)
Competence (7.2)
Awareness and training (7.3)
Communication (7.4)
Documented information (7.5)
CHECK
Monitoring, measurement, analysis and evaluation (9.1)
Internal Audit (9.2)
Management review (9.3)
INTENDED OUTCOMES:
- encouraging and facilitating reporting of wrongdoing;
- supporting and protecting whistleblowers and other relevant stakeholders involved;
- ensuring reports of wrongdoing are dealt with in a proper and timely manner;
- improving organizational culture, governance and the prevention of wrongdoing.

Figure 1 — Overview of a whistleblowing management system

Whistleblowing management systems — Guidelines

1 Scope

This document provides guidance to establish, implement and maintain an effective, responsive whistleblowing management system based on the principles of trust, impartiality and protection in the following four steps:

a) receiving reports of wrongdoing;

b) assessing reports of wrongdoing;

c) addressing reports of wrongdoing;

d) concluding whistleblowing cases.

The guidelines of this document are generic and intended to be applicable to all organizations, regardless of type, size, nature of activity, and whether in the public, private or not-for profit sectors.

The extent of application of this guide depends on the factors specified in 4.1, 4.2 and 4.3. The system can be standalone or can be used as part of an overall management system.

2 Normative references

There are no normative references in this document.

3 Terms and definition

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 https://www.iso.org/obp

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

3.1
management system
set of interrelated or interacting elements of an *organization* (3.2) to establish *policies* (3.7) and *objectives* (3.25) and *processes* (3.28) to achieve those objectives

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

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

Note 3 to entry: The scope of a management system can 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.

3.2
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives (3.25)*

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.

3.3
personnel
organization's (3.2) directors, officers, employees, temporary staff or workers, and volunteers

[SOURCE: ISO 37001:2016 modified by removal of note to entries]

3.4
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 of the organization

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

Note 2 to entry: Stakeholders can include but are not limited to those who make reports, any subjects of those reports, witnesses, personnel, worker representatives, suppliers, third parties, public, media, regulators, and the organization as a whole.

3.5
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 (3.1)* covers only part of the organization, then top management refers to those who direct and control that part of the organization.

3.6
governing body
person or group of people who have ultimate accountability (3.31) for the whole organization (3.2)

Note 1 to entry: Every organizational entity has one governing body, whether or not it is explicitly established.

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

[SOURCE: ISO/IEC 38500:2015, 2.9 amended]

3.7
policy
intentions and direction of an *organization (3.2)*, as formally expressed by its *top management (3.5)*

3.8
wrongdoing
action(s) or omission(s) that can cause harm

Note 1 to entry: wrongdoing can include but is not limited to the following: unethical behavior, fraud, corruption including bribery, breach of law (national or international), breach of the organization's or other relevant code of conduct, gross negligence, breach of organization policy, discrimination, bullying, harassment, unauthorized use of public funds or resources, abuse of authority, conflict of interest, gross waste or mismanagement.

Note 2 to entry: wrongdoing also includes action or omission resulting in damage or risk of harm to: human rights, the environment, public health and safety, safe work-practices or the public interest.

Note 3 to entry: a wrongdoing or the harm can have happened in the past or is currently happening or could happen in the future.

Note 4 to entry: potential harm can be determined by reference to a single event or series of events.

3.9
whistleblower
person who reports wrongdoing (3.8)

3.10
whistleblowing
reporting of wrongdoing (3.8) by a whistleblower (3.9) who has reasonable grounds to believe that the information reported is true at the time of reporting

Note 1 to entry: A report of wrongdoing can be verbal, in person, in writing or in electronic or digital format.

Note 2 to entry: It is common to distinguish:

— open whistleblowing: whistleblower discloses information without withholding their identity or requiring that their identity be kept secret.

— confidential whistleblowing: the identity and any information that can identify the whistleblower is known by the recipient but is not disclosed without the whistleblower’s consent, unless required by legal and/or investigation process.

— anonymous whistleblowing: information is received without the whistleblower disclosing their identity.

Note 3 to entry: organizations may want to use an alternative term such as “speak up” or “raise a concern” or equivalent.

3.11
whistleblowing management function
person(s) with responsibility and authority for the operation of the whistleblowing *management system (3.1)*

3.12
triage
assessment of the initial report of wrongdoing (3.8) for the purposes of categorization, taking preliminary measures, prioritization and allocation

Note 1 to entry: the following factors can be considered: likelihood and severity of impact of wrongdoing on personnel (3.3), *organization (3.2)*, *stakeholders (3.4)* including reputational, financial, environmental, human or other damages.

3.13
detrimental conduct
any threatened, proposed or actual, direct or indirect, act or omission that can result in harm to a whistleblower (3.9) or other relevant party, related to the reporting of wrongdoing (3.8)

Note 1 to entry: Harm includes any adverse consequence, whether work-related or personal, including dismissal, suspension, demotion, transfer, change in duties, alteration of working conditions, adverse performance ratings, reduced opportunity for advancement, denial of services, blacklisting, boycotting, damage to reputation, financial loss, prosecution or legal action, harassment, isolation, or any form of physical or psychological harm.

Note 2 to entry: Detrimental conduct includes retaliation, reprisal, retribution, deliberate action or omissions, done knowingly or recklessly to cause harm to a whistleblower or other relevant parties.

Note 3 to entry: Detrimental conduct also includes the failure to prevent or to minimise harm by fulfilling a reasonable standard of care at any step of the whistleblowing process.

Note 4 to entry: Other relevant stakeholders can include prospective or perceived whistleblowers, relatives, associates of persons who have provided support to a whistleblower, and any person involved in a whistleblowing process including a legal entity.

Note 5 to entry: Action to deal with a whistleblower's own wrongdoing, performance or management, independently of their role in reporting, is not detrimental conduct for the purposes of this standard. However, any such actions will depend on the circumstances of the report and the principles of trust, impartiality and protection underpinning the whistleblowing management system.

3.14
investigation
systematic, independent and documented *process* (*3.28*) for obtaining evidence and evaluating it objectively to determine if wrongdoing has occurred and its extent

Note 1 to entry: An investigation can be an internal investigation or an external investigation, and it can be a combined investigation.

Note 2 to entry: An internal investigation is conducted by the organization itself, or by an external party on its behalf.

Note 3 to entry: An investigation can also be imposed on the organization by external parties.

3.15
audit
systematic, independent and documented *process* (*3.28*) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

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

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

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

3.16
competence
ability to apply knowledge and skills to achieve intended results

3.17
conformity
fulfilment of a *requirement* (*3.29*)

3.18
nonconformity
non-fulfilment of a *requirement* (*3.29*)

3.19
corrective action
action to eliminate the cause of a *nonconformity* (*3.18*) and to prevent recurrence

3.20
continual improvement
recurring activity to enhance *performance* (*3.27*)

3.21
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, from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (*3.1*), including related *processes* (*3.28*);

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

— evidence of results achieved (records).