INTERNATIONAL STANDARD

ISO 37002

First edition
2021-07

Whistleblowing management systems — Guidelines

Systèmes de management des alertes — Lignes directrices

Reference number
ISO 37002:2021(E)

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

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 considering introducing or improving 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 interested parties involved;

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

d) improving organizational culture and governance;

e) reducing the risks 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;
- demonstrating sound, ethical governance practices to society, markets, regulators, owners and other interested parties.

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;
- encouraging a culture of openness, transparency, integrity and accountability.

This document provides guidance for organizations to create a whistleblowing management system based on the 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 can assist an organization to improve its existing whistleblowing policy and procedures, or to comply with applicable whistleblowing legislation.

This document adopts the “harmonized 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 ISO management systems.

Figure 1 is a conceptual overview of a recommended whistleblowing management system showing how the principles of trust, impartiality and protection overlay all elements of such a system.

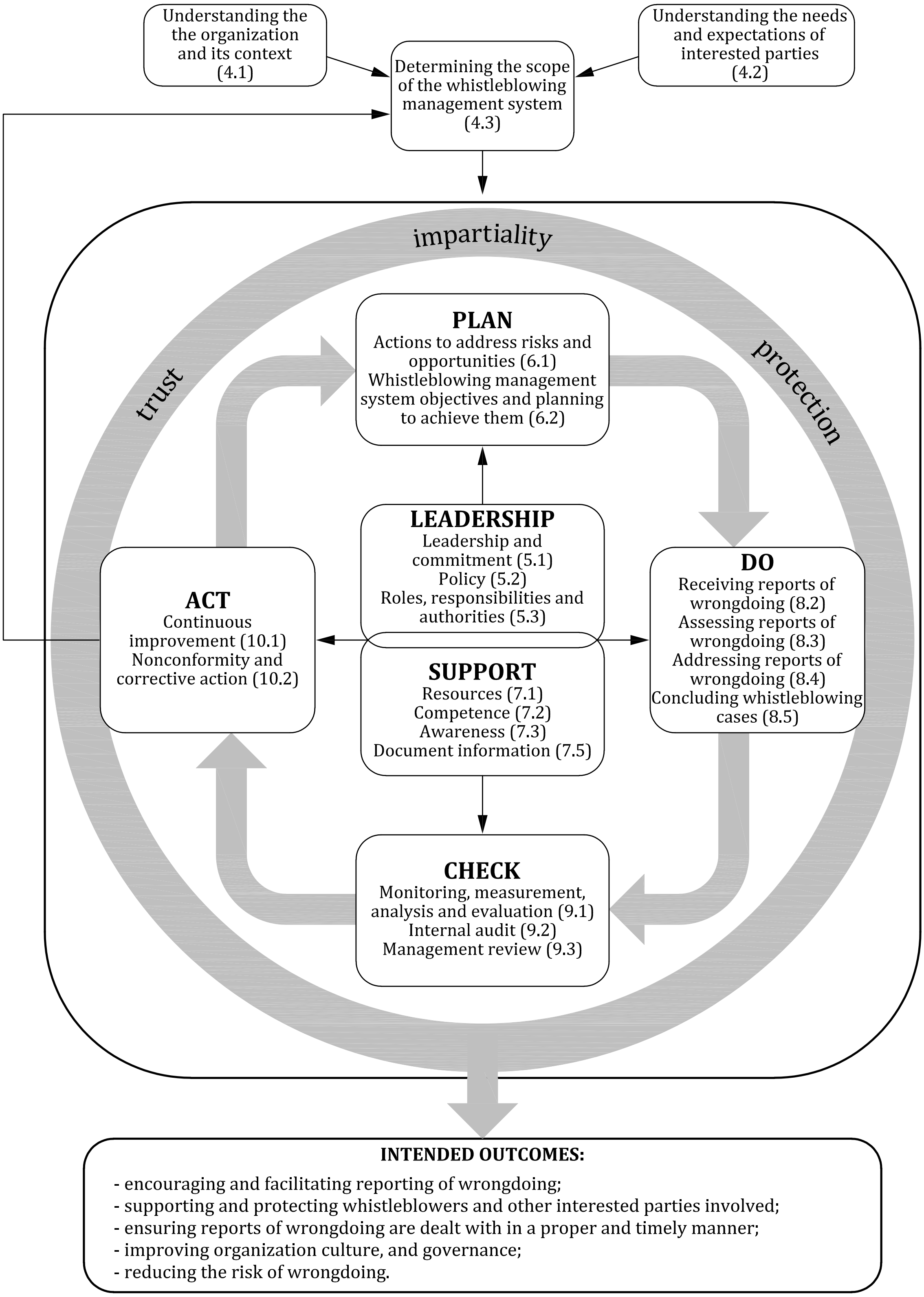
Understanding the the organization and its context (4.1)
Determining the scope of the whistleblowing management system (4.3)
Understanding the needs and expectations of interested parties (4.2)
impartiality
trust
protection
PLAN
Actions to address risks and opportunities (6.1)
Whistleblowing management 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
Continuous improvement (10.1)
Nonconformity and corrective action (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 (7.3)
Document 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 interested parties involved;
- ensuring reports of wrongdoing are dealt with in a proper and timely manner;
- improving organization culture, and governance;
- reducing the risk of wrongdoing.

Figure 1 — Overview of a whistleblowing management system

Whistleblowing management systems — Guidelines

1 Scope

This document gives guidelines for establishing, implementing and maintaining an effective 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 these guidelines depends on the factors specified in 4.1, 4.2 and 4.3. The whistleblowing management system can be stand-alone 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 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 https://www.iso.org/obp

— IEC Electropedia: available at https://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), as well as *processes* (3.27) 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: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

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.

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 *whistleblowing* (3.10) *management system* (3.1).

Note 3 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

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

[SOURCE: ISO 37001:2016, 3.25, modified — Notes 1 and 2 to entry have been deleted.]

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

Note 1 to entry: An interested party can be internal or external to the organization.

Note 2 to entry: Interested parties can include, but are not limited to, those who make reports, any subjects of those reports, witnesses, *personnel* (3.3), worker representatives, suppliers, third parties, public, media, regulators and the organization as a whole.

Note 3 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards. The original definition has been modified by adding Notes 1 and 2 to entry.

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 an organization, then top management refers to those who direct and control that part of the organization.

Note 3 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.6
governing body
person or group of people who have ultimate *accountability* (3.30) 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, a board of directors, committees of the board, a supervisory board or trustees.

[SOURCE: ISO/IEC 38500:2015, 2.9, modified — The words "have ultimate accountability for" have replaced "accountable for the performance and conformance of" and Notes 1 and 2 to entry have been added.]

3.7
policy

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

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

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:

- breach of law (national or international), such as fraud, corruption including bribery;
- breach of the *organization's* (3.2) or other relevant code of conduct, breach of organization *policies* (3.7);
- gross negligence, bullying, harassment, discrimination, unauthorized use of funds or resources, abuse of authority, conflict of interest, gross waste or mismanagement;
- actions or omissions resulting in damage or risk of harm to human rights, the environment, public health and safety, safe work-practices or the public interest.

Note 2 to entry: Wrongdoing or the resulting harm can have happened in the past, is currently happening or can happen in the future.

Note 3 to entry: Potential harm can be determined by reference to a single event or series of events.

3.9
whistleblower

person who reports suspected or actual *wrongdoing* (3.8), and has reasonable belief that the information is true at the time of reporting

Note 1 to entry: Reasonable belief is a belief held by an individual based on observation, experience or information known to that individual, which would also be held by a person in the same circumstances.

Note 2 to entry: Examples of whistleblowers include, but are not limited to, the following:

- *personnel* (3.3) within an *organization* (3.2);
- personnel within external parties, including legal persons, with whom the organization has established, or plans to establish, some form of business relationship including, but 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;
- other persons such as union representatives;
- any person formerly or prospectively in a position set out in this definition.

3.10
whistleblowing

reporting of suspected or actual *wrongdoing* (3.8) by a *whistleblower* (3.9)

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

Note 2 to entry: It is common to distinguish:

- open whistleblowing, where the whistleblower discloses information without withholding their identity or requiring that their identity be kept secret;
- confidential whistleblowing, where the identity of the whistleblower and any information that can identify them is known by the recipient but is not disclosed to anyone beyond a need to know basis without the whistleblower's consent, unless required by law;
- anonymous whistleblowing, where information is received without the whistleblower disclosing their identity.

Note 3 to entry: *Organizations* (3.2) can use an alternative term such as “speak up” or “raise a concern”, or an equivalent.

3.11
whistleblowing management function

person(s) with the responsibility and authority for the operation of the *whistleblowing* (3.10) *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 assignment for further handling

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

3.13
detrimental conduct

threatened, proposed or actual, direct or indirect act or omission that can result in harm to a *whistleblower* (3.9) or other relevant *interested party* (3.4), related to *whistleblowing* (3.10)

Note 1 to entry: Harm includes any adverse consequence, whether work-related or personal, including, but not limited to, dismissal, suspension, demotion, transfer, change in duties, alteration of working conditions, adverse *performance* (3.26) ratings, disciplinary proceedings, reduced opportunity for advancement, denial of services, blacklisting, boycotting, damage to reputation, disclosing the whistleblower’s identity, financial loss, prosecution or legal action, harassment, isolation, imposition of 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 minimize harm by fulfilling a reasonable standard of care at any step of the whistleblowing *process* (3.27).

Note 4 to entry: Action to deal with a whistleblower’s own *wrongdoing* (3.8), performance or management, unrelated to their role in whistleblowing, is not detrimental conduct for the purposes of this document.

Note 5 to entry: Other relevant interested parties can include prospective or perceived whistleblowers, relatives, associates of a whistleblower, persons who have provided support to a whistleblower, and any person involved in a whistleblowing process, including a legal entity.

3.14
investigation

systematic, independent and documented *process* (3.27) for establishing facts and evaluating them objectively to determine if *wrongdoing* (3.8) has occurred, is occurring or is likely to occur, and its extent

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

Note 2 to entry: An internal investigation is conducted by the *organization* (3.2) 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 and independent *process* (3.27) 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.

Note 4 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

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

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.17
conformity
fulfilment of a *requirement* (3.28)

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.18
nonconformity
non-fulfilment of a *requirement* (3.28)

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

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

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.20
continual improvement
recurring activity to enhance *performance* (3.26)

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

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, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.1), including related *processes* (3.27);

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

— evidence of results achieved (records).

Note 3 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.22
effectiveness
extent to which planned activities are realized and planned results are achieved

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.23
measurement
process (3.27) to determine a value

Note 1 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.24
monitoring
determining the status of a system, a *process* (3.27) or an activity

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

Note 2 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.25
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, health and safety and environment) They can be, for example, organization-wide or specific to a project, product, service or *process* (3.27).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, a purpose, an operational criterion, as a *whistleblowing* (3.10) 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 whistleblowing *management systems* (3.1), whistleblowing objectives are set by the *organization* (3.2), consistent with the whistleblowing *policy* (3.7), to achieve specific results.

Note 5 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.26
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* (3.27), products, services, systems or *organizations* (3.2).

Note 3 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.27
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 output, product or service depends on the context of the reference.

Note 2 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.28
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.2) and *interested parties* (3.4) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.21).

Note 3 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards.

3.29
risk
effect of uncertainty on *objectives* (3.25)

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) and consequences (as defined in ISO Guide 73), 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) of occurrence.

Note 5 to entry: This constitutes one of the common terms and core definitions of the harmonized structure for ISO management system standards. The original definition has been modified by adding "on objectives" to the definition.

3.30
accountability
obligation to another for the fulfilment of a responsibility

4 Context of the organization

4.1 Understanding the organization and its context

The organization should determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its whistleblowing management system.

These issues may include, but are not limited to, the following factors:

a) the size and structure of the organization;

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

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

d) the nature and needs of personnel;

e) the organization's business model;

f) the entities over which the organization has control and entities which exercise control over the organization, including beneficial owner(s) of the organization;

g) the organization's business associates;

h) the organization's exposure to public interest obligations or issues;

i) applicable statutory, regulatory, contractual and other obligations and duties.

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

4.2 Understanding the needs and expectations of interested parties

The organization should determine:

a) the interested parties that are relevant to the whistleblowing management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the whistleblowing management system.

4.3 Determining the scope of the whistleblowing management system

The organization should determine the boundaries and applicability of the whistleblowing management system to establish its scope.

When determining this scope, the organization should consider:

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

b) the requirements referred to in 4.2;

c) who can report (internal/external interested parties), from where (regions/geographic) and what types of wrongdoing are covered by the system (see Figure 2);

d) the outcomes of any compliance risk assessment or equivalent, as available.

Organizations can reference ISO 37301 for compliance risk assessment and ISO 31000 for risk management.

The types of wrongdoing that can be addressed through the whistleblowing management system, if reported, are important to its scope. Not all reports made to the whistleblowing management system will be within its scope, and a single report can include information about multiple types of wrongdoing, some within scope and others outside of scope. The organization should identify what other processes, existing or planned, will be used to resolve reported wrongdoing that is not within the scope of the whistleblowing management system (e.g. complaints, grievances) and how this will be coordinated.

This is illustrated in Figure 2.

The scope should be available as documented information.

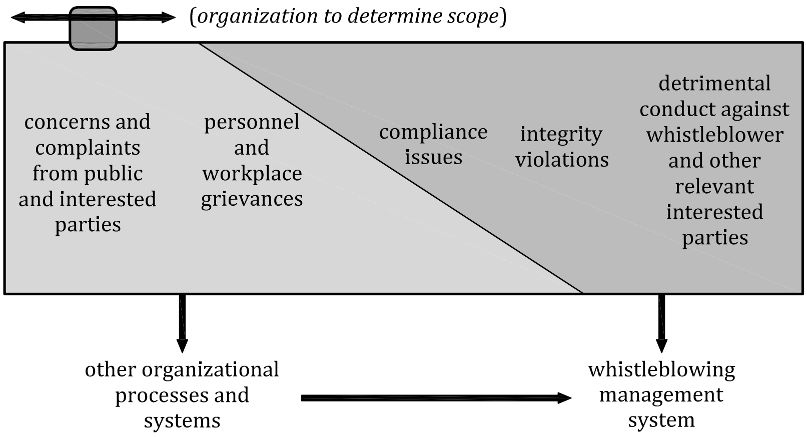
(*organization to determine scope*)
concerns and complaints from public and interested parties
personnel and workplace grievances
compliance issues
integrity violations
detrimental conduct against whistleblower and other relevant interested parties
other organizational processes and systems
whistleblowing management system

Figure 2 — Relationship between the whistleblowing management system and other organizational processes and systems

4.4 Whistleblowing management system

The organization should establish, implement, maintain and continually improve a whistleblowing management system, including the processes needed and their interactions, in accordance with the recommendations of this document.

The whistleblowing management system should apply the principles of trust, impartiality and protection, and should ensure appropriate feedback throughout the entire process. The whistleblowing management system should support all steps of the whistleblowing process.

a) Receiving reports of wrongdoing: the whistleblowing management system should specify how reports can be made and received, taking into consideration the factors included in 4.3.

b) Assessing reports of wrongdoing (triage): the whistleblowing management system should specify the process of assessing received reports, including aspects such as priority, completeness and relevance of the information. At the same time, the whistleblowing management system should provide for an assessment of the risk of detriment to and the level of protection and support required for whistleblowers and others involved.

c) Addressing reports of wrongdoing: the whistleblowing management system should provide for an impartial and timely investigation, as well as effective and timely protective and support measures and monitoring as appropriate for the whistleblower and others involved, including those who are subject of the report. Those protective measures can prevent and contain, as well as remediate detriment.

d) Concluding whistleblowing cases**:** the whistleblowing management system should provide a mechanism to close investigations and take action in response to recommendations and decisions based on the outcomes of the addressing step. It should also ensure that protective and support measures can continue and will be monitored as appropriate. Outcomes may be used for management reporting, organizational learning and other actions (e.g. mitigation remedies).

The steps of the whistleblowing process are specified in 8.2 to 8.5.

5 Leadership

5.1 Leadership and commitment

5.1.1 Governing body

The governing body should:

a) set objectives for an effective whistleblowing management system and monitor top management with respect to these;

b) approve the organization’s whistleblowing policy and communicate clear messages about its existence, importance and use;

c) demonstrate that commitment by embracing the policy and the whistleblowing management system;

d) at planned intervals, receive and review information about the content and operation of the organization’s whistleblowing management system;

e) ensure that adequate and appropriate resources needed for effective operation of the whistleblowing management system are allocated and assigned;

f) exercise adequate oversight of the implementation, integrity and improvement of the organization’s whistleblowing management system.

5.1.2 Top management

Top management should demonstrate leadership and commitment with respect to the whistleblowing management system by:

a) ensuring that the whistleblowing policy and whistleblowing management system objectives are established and are compatible with the values, objectives and strategic direction of the organization;

b) approving the organization’s whistleblowing policy;

c) ensuring the accessibility of the whistleblowing management system and encouraging its use;

d) ensuring the integration of the whistleblowing management system requirements into the organization’s business processes, including management systems;

e) ensuring that the resources needed for the whistleblowing management system are available, adequate, appropriate and deployed;

f) communicating the importance of effective whistleblowing management and of conforming to the organization’s established whistleblowing management system requirements;

g) communicating the whistleblowing policy internally and externally (see 7.4);

h) ensuring that the whistleblowing management system achieves its intended result(s) (see 6.1);

i) directing and supporting persons to contribute to the effectiveness of the whistleblowing management system;

j) promoting continual improvement;

k) supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility;

l) committing to, promoting and practising a speak-up/listen-up culture within the organization, e.g. by actively participating in relevant staff training sessions and, with their consent, publicly commending organization’s whistleblowers;

m) ensuring that whistleblowers and others involved will not suffer detriment by the organization in relation to whistleblowing;

n) at planned intervals, receiving and reviewing reports on the operation, and performance of, the whistleblowing management system;

o) ensuring an impartial investigation of matters reported using the system, regardless of the identity of the whistleblower, the subject of the report and the implications of the issues identified.

NOTE 1 Reference to “business” in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization’s existence.

NOTE 2 A speak-up/listen-up culture means to provide a trustworthy two-way environment where any relevant party is sufficiently confident and encouraged to raise concerns about wrongdoing or suspected wrongdoing, and the organization demonstrates its commitment to receiving, assessing, addressing and concluding whistleblowing cases.

Trustworthiness of the whistleblowing management system depends on whether interested parties perceive that management is committed to the system and will follow procedures.

5.2 Whistleblowing policy

Top management should establish a whistleblowing policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting whistleblowing management system objectives;

c) explains the scope of the whistleblowing management system (see 4.3);

d) includes a commitment to meet applicable requirements;

e) includes a commitment to the continual improvement of the whistleblowing management system;

f) prohibits detrimental conduct;

g) clearly commits to a speak-up/listen-up culture;

h) provides guidance, in easily understandable language, on how to report and where to seek support or advice on the whistleblowing process;

i) includes a commitment to trust, impartiality and protection throughout the whistleblowing process;

j) provides for the protection of confidentiality in reporting of wrongdoing;

k) explains the authority and independence of the whistleblowing management function;

l) explains the consequences of non-compliance with the whistleblowing policy, e.g. making knowingly false reports and taking detrimental conduct can warrant disciplinary action;

m) makes reference to alternative reporting channels available outside the organization, such as regulators;

n) makes reference to applicable law;

o) outlines key steps of the whistleblowing management systems, including how reports will be received, assessed, addressed and concluded;

p) does not restrict reporting based on contractual obligations such as non-disclosure agreements, or clauses such as commercial-in-confidence and employee-in-confidence, etc.;

q) provides information about the organization’s data retention policy.

The whistleblowing policy should:

- be developed in participation with personnel and other interested parties, as appropriate;
- be in line with other policies;
- be readily available as documented information;
- be regularly communicated in appropriate languages within and outside the organization;
- be available to interested parties, as appropriate, with due regard to aspects such as age, language, disabilities, etc.;
- be reviewed at planned intervals.

5.3 Roles, responsibilities and authorities

5.3.1 Top management and governing body

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

Top management should assign the responsibility and authority to the whistleblowing management function for:

a) ensuring that the whistleblowing management system conforms to the recommendations of this document;

b) reporting on the performance of the whistleblowing management system to the governing body and top management.

Top management can assign some or all of the whistleblowing management function to persons external to the organization. If it does, top management should ensure that designated personnel within the organization have responsibility for, and authority over, those externally assigned parts of the function.

The governing body, top management and all other personnel should be responsible for understanding, conforming to and applying the whistleblowing management system recommendations, as it relates to their role in the organization.

5.3.2 Whistleblowing management function

The whistleblowing management function should have the responsibility and authority for:

a) the design, implementation, operation and improvement of the whistleblowing management system;

b) ensuring that the whistleblowing management system is designed and resourced to ensure comprehensive assessment of reports and the risks of detriment, impartial and timely investigations of reports and protection and support arrangements;

c) ensuring, to the maximum extent possible in the organization, that investigation and protection functions are delivered independently (i.e. provided by different persons or areas), while recognizing that each may be assigned to existing functions;

d) providing advice and guidance on the whistleblowing management system and issues relating to reporting wrongdoing;

e) reporting on a planned and ad hoc basis on the performance of the whistleblowing management system to the governing body, top management and other relevant functions, such as the compliance function, as appropriate.

The whistleblowing management function should be adequately resourced (see 7.1) and assigned to personnel who have the appropriate competence (see 7.2), integrity, authority and independence. This should include direct, unrestricted access to adequate resources as necessary to ensure the impartiality, integrity and transparency of the whistleblowing management system and its processes.

The whistleblowing management function should have direct, unrestricted and confidential access to top management and the governing body.

NOTE Organizations that do not have a person dedicated solely to this function can appoint one or more persons to fulfil that function, in addition to other responsibilities, as long as there are no conflicts of interests or trust and impartiality issues.

5.3.3 Delegated decision-making

Top management can delegate authority for decisions as part of the whistleblowing process, such as receiving the reports of wrongdoing, making assessments, implementing protection and support arrangements, conducting investigations and concluding cases. The organization should establish and maintain an appropriate decision-making process (including policies and controls) which includes that decision-makers have an appropriate level of authority and are free of actual or potential conflicts of interest.

Top management should ensure that these processes are reviewed periodically as part of its role and responsibility for the implementation of, and compliance with, the whistleblowing management system.

6 Planning

6.1 Actions to address risks and opportunities

When planning for the whistleblowing management system, the organization should consider its existing policies, processes and functions (compliance, legal, reporting, procurement, disclosure, communication etc.), the issues referred to in 4.1 and the needs and expectations referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

- give assurance that the whistleblowing management system can achieve its intended result(s), i.e.:
  - encourage and facilitate reporting of wrongdoing;
  - support and protect whistleblowers and other relevant interested parties involved;
  - ensure reports of wrongdoing are dealt with in a proper and timely manner;
  - improve organizational culture and governance;
  - reduce the risks of wrongdoing;
- prevent, or reduce, undesired effects;
- achieve continual improvement.

The organization should plan:

a) actions to address these risks and opportunities;

b) how to:
   - integrate and implement the actions into its whistleblowing management system processes;
   - evaluate the effectiveness of these actions;
   - involve relevant personnel and relevant interested parties in the planning of the whistleblowing management system;
   - address instances where wrongdoing is reported outside the organization (e.g. to relevant authorities);
   - define the degree of confidentiality, support and protection that the organization can provide within the whistleblowing management system;
   - provide feedback to and collect feedback from the whistleblower and other relevant interested parties.

6.2 Whistleblowing management system objectives and planning to achieve them

The organization should establish its whistleblowing management system objectives at relevant functions and levels.

The whistleblowing management system objectives should:

a) be consistent with the whistleblowing policy;

b) be measurable (if practicable);

c) take into account applicable requirements;

d) be monitored;

e) be evaluated;

f) be communicated;

g) be updated and/or revised as appropriate;

h) ensure the early detection and prevention of wrongdoing;

i) be available as documented information.

When planning how to achieve its whistleblowing management system objectives, the organization should determine:

- what will be done;
- what resources will be required;
- who will be responsible;
- when it will be completed;
- how the results will be monitored and evaluated;
- how it will be updated as appropriate;
- how the results will be communicated.

6.3 Planning of changes

When the organization determines the need for changes to the whistleblowing management system, the changes should be carried out in a planned manner (see 10.1).

7 Support

7.1 Resources

The organization should determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the whistleblowing management system and in meeting its objectives.

Resources may include, but are not limited to, financial and human resources, IT solutions, specialized skills, organizational infrastructure, investigators, contemporary reference material on whistleblowing, legal expertise, and professional development and training. These resources may be provided internally or externally.

NOTE Depending on the organization's size, complexity, structure, operations and other considerations referred to in 4.1, 4.2 and 4.3, organizations can outsource certain functions of the whistleblowing management system. Organizations can outsource the collection, processing and investigation of whistleblower reports to independent third parties or external service providers such as whistleblowing solution providers, consulting services, organization's ombudsman, etc. However, if the organization wishes to handle all of these aspects internally, it can do so also in consideration of the possible limitations and constraints caused by its size and structure.

7.2 Competence

The organization should:

- determine the necessary competence of person(s) doing work under its control that affects the whistleblowing management system, its performance and operations;

- ensure that these persons are competent on the basis of appropriate education, training, or experience;
- ensure that, where relevant, the personnel are able to work with the appropriate level of impartiality;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

Appropriate documented information should 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 currently employed persons; or the hiring or contracting of competent persons.

Those responsible for carrying out activities related to protection, support and investigation should display, among others, the following characteristics:

- trustworthiness;
- emotional intelligence;
- diplomacy;
- impartiality;
- integrity;
- leadership;
- confidentiality;
- sound judgement.

7.3 Awareness

7.3.1 General

Persons doing work under the organization's control should be aware of:

- the whistleblowing policy (see 5.2);
- the whistleblowing management system objectives (see 6.2);
- their contribution to the effectiveness of the whistleblowing management system, including the benefits of improved performance of the whistleblowing management system (see 10.2);
- the implications of not conforming with the whistleblowing management system requirements.

7.3.2 Personnel training and awareness measures

The organization should provide appropriate awareness measures and training to personnel. Such training should address the following issues:

a) the organization's whistleblowing management system, policy, processes, procedures, tools and duty to comply;

b) their contribution to the effectiveness of the whistleblowing management system;

c) how to recognize wrongdoing;

d) how and to whom they can report suspected wrongdoing;

e) how and to whom they can ask questions regarding the whistleblowing management system;

f) how they can help prevent, avoid and protect from detrimental conduct;

g) information on available support and resources;

h) the protections available when using the whistleblowing management system;

i) the provisions provided for under relevant local legislation;

j) the impact of not reporting wrongdoing and its potential consequences;

k) information for potential whistleblowers about independent confidential advice available

l) the organization's code of conduct or code of ethics or equivalent where it exists;

m) explain the consequences of non-compliance with the whistleblowing policy, e.g. how making knowingly false reports and detrimental conduct can warrant disciplinary action;

All personnel should understand that:

— while it can often be desirable or necessary for individuals to first report wrongdoing to their manager, it can also be desirable or necessary to report wrongdoing via other channels provided by the organization, especially if a manager fails to act appropriately or is conflicted;

— the whistleblowing policy is not a substitute for managers taking responsibility for their workplace;

— the whistleblowing management system provides complementary reporting channels and protections, and managers are instrumental to its implementation;

— the whistleblowing policy does not prevent an individual reporting to the relevant authorities;

— the whistleblowing management system is not a substitute for local legal obligations to report to the relevant authorities, when applicable.

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

The organization should implement procedures addressing awareness measures and training for business associates acting on its behalf or for its benefit. These procedures should identify the business associates for which such awareness measures and training is necessary, its content and the means by which the training should be provided.

The organization should retain documented information that training has taken place.

7.3.3 Training for leaders and other specific roles

The governing body, top management, the whistleblowing management function, managers and any person(s) having roles, responsibilities and authorities within the whistleblowing management system should be trained in the operation of the policy and in how to handle reports of wrongdoing.

Training should cover such issues as:

a) the scope of wrongdoing within the whistleblowing policy;

b) what is wrongdoing and what is not;

c) channels to report wrongdoing;

d) what a whistleblower can expect from the whistleblowing policy, in terms of communication and processes, and how the report of wrongdoing will be assessed and addressed;

e) what processes are in place to ensure trust, impartiality and protection;

f) what confidentiality is, its importance and how to maintain it;

g) the concept and types of detrimental conduct(s), how to prevent it and address it, including what the consequences are for the person responsible for it and remediation available for the person that suffered from detrimental conduct.;

h) how to receive reports of wrongdoing;

i) how to assess reports of wrongdoing;

j) how to address reports of wrongdoing;

k) how to give feedback to the whistleblower;

l) what interactions with whistleblowers can look like and how to respond appropriately;

m) the importance of a fair and impartial investigation, including that the subjects of the reports are presumed innocent;

n) how and when corrective actions should be taken;

o) the implications when reports of wrongdoing are not managed in compliance with the whistleblowing policy;

p) how to make and keep (i.e. retaining or maintaining, as appropriate) documentation relating to the whistleblowing management system.

7.4 Communication

The organization should determine the internal and external communications relevant to the whistleblowing management system, including:

a) on what it will communicate;

b) when to communicate;

c) with whom to communicate;

d) how to effectively communicate;

e) who communicates;

f) the language(s) in which to communicate.

When the policy is introduced or updated, the following actions should be taken.

- Personnel should be briefed on the key points/changes. The involvement of their managers:
  - helps ensure that managers have a clear role in the arrangements and their role is widely understood;
  - communicates the message from managers themselves that it is safe and acceptable for their personnel to report wrongdoing by those above them.
- A communication should be sent from the governing body or top management (e.g. personalized letter, a newsletter or a post on the intranet, etc.). This will give the initiative credibility across the organization and is an effective way to demonstrate leadership (see 5.1).

Organizations should consider to what extent other interested parties should receive this communication.

The whistleblowing policy and information on the whistleblowing management system should be effectively communicated to new personnel and included, when it exists, in the new employee information package delivered when joining the organization.

The organization should use its usual communication channels, such as newsletters, email, posters, intranet or internet posts, personnel meetings, town halls, training courses, internal bulletin boards or hand-held flyers, brochures, wallet cards, social media, in person and any other appropriate communications vehicles.

7.5 Documented information

7.5.1 General

The organization's whistleblowing management system should include:

a) documented information recommended by this document;

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

NOTE The extent of documented information for a whistleblowing management system can differ from one organization to another due to:

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

— the complexity of processes and their interactions;

— the competence of persons.

7.5.2 Creating and updating documented information

When creating and updating documented information, the organization should ensure appropriate:

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

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

— review and approval for suitability and adequacy;

— data protection measures.

NOTE It is helpful to set up a regular review system of all unresolved reports, depending on the size and complexity of the organization. In addition, ensuring that all cases are dealt with in accordance with the whistleblowing policy is helpful to identify trends and areas for improvement.

7.5.3 Control of documented information

Documented information required by the whistleblowing management system and recommended by this document should 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 should 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 whistleblowing management system should be identified as appropriate, and controlled.

The whistleblowing management function should ensure documented information is kept and maintained in accordance with the organization's data retention policy (see also data protection in 7.5.4), including:

- all reports of wrongdoing, as outlined in 8.2;
- action taken;
- outcomes of investigations undertaken;
- other relevant documentation.

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.

7.5.4 Data protection

Data protection should be considered as it can have an impact on identified aspects of the whistleblowing management system. Examples of impacted areas include, but are not limited to, the following:

a) identification of who can access the relevant data and who approves such access;

b) data management (security, retention, deletion, access, modification of personal identifiable information and international data transfers);

c) data protection rights of the whistleblower, any subject(s) of the report and other interested parties implicated in the wrongdoing;

d) notice regarding collected data;

e) whistleblowing management system scope;

f) whether anonymity is permitted or not.

When an organization is considering outsourcing to an external whistleblowing provider, sufficient due diligence should be done to ensure the highest available data protection standards are applicable by default and by design.

7.5.5 Confidentiality

Processes should be put in place to ensure that all interested parties including the whistleblower and any subjects of the report are afforded confidentiality. The identity of the whistleblower and relevant interested parties should not be disclosed to anyone beyond a need-to-know basis without their consent. Where it is likely that a whistleblower's identity is known (because they have previously openly raised concerns or the nature of the information means they are easily identifiable) or needs to be revealed by law, the whistleblower should be notified beforehand, and potentially additional steps should be taken to protect them from detriment.

When establishing processes, including procedures and tools, to ensure the confidentiality of a whistleblower and other interested parties implicated in the whistleblowing process, including any subject(s) of the report, organizations should consider the following:

a) a number of characteristics can inadvertently identify a person (name, voice, gender, job description, department, etc.);

b) the circumstances of the reported wrongdoing can inadvertently lead to the identification of the whistleblower;

c) the way an organization investigates the report of wrongdoing can also inadvertently identify the whistleblower;

d) the way an outcome is reported can also identify the whistleblower;

e) the way an organization collects data on indicators for evaluation (9.1.2) can inadvertently identify whistleblowers who have reported confidentially;

f) making whistleblowers aware that when confidential or anonymous reporting is allowed, disclosing their identity during the investigation can be required to proceed further;

g) making whistleblowers aware that when anonymous reporting is allowed, anonymous reporting can limit the ability to both investigate and protect the individual;

h) when anonymity is permitted, organizations may define mechanisms to enable communication with the whistleblower.

Procedures should include how to deal with instances where confidentiality has been breached or an attempt has been made to identify the whistleblower or relevant interested parties. This includes providing support and taking disciplinary measures.

8 Operation

8.1 Operational planning and control

Organizations should ensure their whistleblowing management system includes the following processes as shown in Figure 3:

- receiving reports of wrongdoing;
- assessing how best to deal with reports of wrongdoing, and protect and support the whistleblower;
- addressing the reports of wrongdoing, and the protection and support needs of persons involved;
- concluding whistleblowing cases.

Providing feedback to whistleblowers can help to build and maintain trust, and provide an opportunity for the whistleblower to communicate additional information. Feedback should manage expectations and be made in an empathetic tone. It should include:

a) information about the status of the report;

b) next steps (if any).

Feedback should be provided at each step of the whistleblowing process (see Figure 3).

Acknowledgement of receipt should be timely (for example an immediate automated acknowledgement of receipt, followed by a personalised message within three working days). If a particular step is taking longer than expected, intermediate feedback should be made to the whistleblower to update the time frame.

The level of detail provided to the whistleblower on actions taken by the organization as a result of the whistleblowing that can be given in feedback can be limited to avoid compromising any investigation.

EXAMPLE Feedback can include:

- reassurance [e.g. “thank you, we are taking your report seriously” (receipt); “information is useful however [question]” (assessment); “we will start an investigation, would you be happy to talk to an investigator directly?” (assessment); “Do you want to provide additional information?” (assessment)];

- establish channels for further communication (offer possibility to continue or change way of communicating, e.g. report was made online but whistleblower prefers to continue in person);
- next steps in the process and possible outcomes;
- time frame for next steps (when can they expect further feedback);
- reasons for the limited detail of feedback;
- information on available support and measures taken for their protection, including measures to protect their identity or their anonymity;
- information on the responsibilities of the organization;
- information on the responsibilities of the whistleblower.

Organizations should ensure that each step of the whistleblowing process is started without undue delay and is completed within a reasonable time frame (see Figure 3).

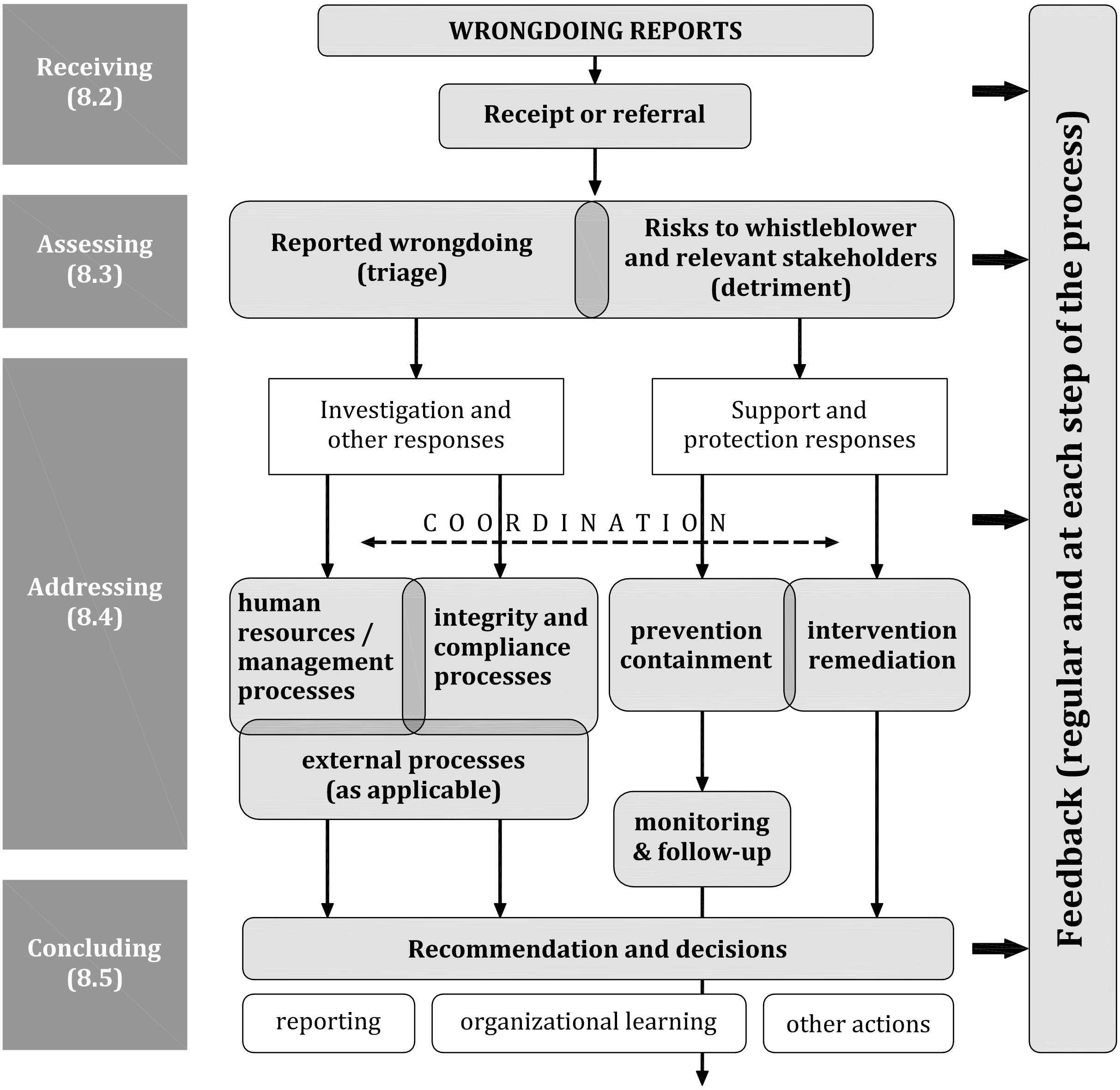
Receiving (8.2)
Assessing (8.3)
Addressing (8.4)
Concluding (8.5)
WRONGDOING REPORTS
Receipt or referral
Reported wrongdoing (triage)
Risks to whistleblower and relevant stakeholders (detriment)
Investigation and other responses
Support and protection responses
COORDINATION
human resources / management processes
integrity and compliance processes
prevention containment
intervention remediation
external processes (as applicable)
monitoring & follow-up
Recommendation and decisions
reporting
organizational learning
other actions
Feedback (regular and at each step of the process)

Figure 3 — Operational steps of the whistleblowing management system

The organization should plan, implement and control the processes needed to meet recommendations, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

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

The organization should control planned changes (see 6.3) and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization should ensure that externally provided processes, products or services, that are relevant to the whistleblowing management system are controlled.

8.2 Receiving reports of wrongdoing

Organizations should identify, implement, communicate and maintain visible, accessible and secure reporting channels. To the extent possible, at least one channel should be distinct from the management hierarchy. Reporting channels can be alternative internal reporting channels or reporting channels operated by an outsourced whistleblowing service provider.

NOTE Visible and accessible means that whistleblowers can easily find and use the available reporting channels.

Common methods for receiving reports can include in person conversations, the use of internal or external telephone lines, online, email, digital or mobile application reporting, by post or internal letterbox.

EXAMPLE 1 In person channels, including reporting to different management functions (e.g. line manager, top management, governing body, data protection officer, environmental and/or health safety officer, compliance officer or an organization’s ombudsman):

— ensure conversations are held in a location where confidentiality is ensured;

— clarify and capture more useful information from the whistleblower, as well as build trust and rapport.

EXAMPLE 2 For telephone channels, the following elements can increase accessibility and trustworthiness:

— dedicated toll-free number;

— multi-language capable where relevant;

— availability outside the normal business hours of the organization;

— use of a human operator, who can clarify and capture more useful information from the whistleblower as well as build trust and rapport;

— a physically secure location for operators, which can also increase confidentiality;

— that the conversation is not recorded without the consent of the whistleblower.

EXAMPLE 3 Web-based online, digital or mobile application reporting channels can:

— facilitate two-way secured anonymous or confidential communication;

— offer the whistleblower the option to upload attachments;

— be multi-language capable where relevant.

EXAMPLE 4 Reports by post can be directed to a dedicated address that is treated securely. When internal letter boxes are used as a channel in a whistleblowing management system, it is important that organizations ensure they are able to maintain anonymity or confidentiality, e.g. that they are not in range of any security camera to avoid inadvertently identifying the whistleblower.

Regardless of the channel:

- organizations may suggest a structure of a report without being prescriptive;
- information should be treated as in accordance with 7.5.

Managers should be trained to appropriately identify and deal with reports of wrongdoing (see 7.3).

NOTE Information to ask the whistleblower can include the following.

- Where did the wrongdoing take place (jurisdiction)?
- When did the wrongdoing take place (past, current, future, ongoing)?
- Who is involved in the wrongdoing?
- Have you reported this previously? If so, what, when and to whom? What action did they take?
- What is the impact for the organization from your view?
- Is management involved or aware of the wrongdoing?
- Are there any risks to you or others?
- Do you have any documents or other evidence such as pictures to support the report?
- Is there anyone else with first-hand knowledge we can contact?
- Have I understood your concerns correctly?
- Has anyone tried to hide this, or tried to discourage you from sharing your concern? If so, please tell us who, and how.

The whistleblower's expectations should be managed. Whistleblowers should not be asked to proactively gather further evidence of wrongdoing. The whistleblower should be informed about what can be expected in terms of feedback, time of response, operational and legal provisions and limitations (e.g. scope, confidentiality and anonymity). An appropriate channel for further communication should be agreed with the whistleblower.

8.3 Assessing reports of wrongdoing

8.3.1 Assessing the reported wrongdoing

The organization should identify, implement and maintain (a) process(es) that ensure(s) the impartial assessment, triage and management of the reports of wrongdoing(s). The assessment decisions should be documented (see 7.5).

Reports should be sorted and prioritized based on risk (i.e. the likelihood of the wrongdoing and its potential impact).

NOTE When assessing reports, the following aspects can be considered.

- Is the wrongdoing within the scope of the whistleblowing policy? If not, does it need to be dealt with in accordance with another procedure or addressed in another way (see 4.3)?
- Is the wrongdoing a criminal offence? Does the wrongdoing need to be referred to law enforcement or regulatory authorities?
- When did the wrongdoing happen or is it about to happen?
- Is there an immediate need to stop or suspend business activities?
- Is there an immediate risk to health and safety?
- Is there an immediate risk to human rights or the environment?

- Is there an immediate need to secure and protect evidence before being deleted or destroyed?
- Is there a risk to the organization's functions, services and/or reputation?
- Will business continuity be affected by the report being investigated?
- Could there be media interest in the report of wrongdoing?
- How can this assessment process be managed, while ensuring trust, protection and impartiality?
- Is further corroborating information available?
- What is the nature of the wrongdoing (i.e. type, frequency, prevalence, role and seniority of subjects of the reports)?
- What is the likelihood of the wrongdoing being reported outside of the organization?
- Has the wrongdoing been reported previously?
- How did the whistleblower obtain the information: is the information first-hand or hearsay?

The outcome of assessing the report of wrongdoing may include doing one or more of the following:

a) engage with other functions (e.g. human resources, legal, internal audit, compliance, health and safety, finance), if needed, and if this does not compromise the trust, impartiality and protection of the investigation, to support the investigation;

b) gather further information;

c) take preliminary measures (e.g. suspension of the subject of the report, secure evidence);

d) investigate the report of wrongdoing;

e) refer to or coordinate with other procedures;

f) inform relevant authorities (e.g. law enforcement or regulatory body);

g) conclude the case (see 8.5).

The decision, and where possible the reasons for it, should be communicated to the whistleblower (see 8.1).

8.3.2 Assessing and preventing risks of detrimental conduct

When a report is made, organizations should assess the risk of detriment to the whistleblower and other relevant interested parties, by considering for example the following.

a) What is the likelihood of confidentiality being maintained? (e.g. Who else knows? Who else have they told? Does the nature of the information reveal their identity? Are they the only person who has access to the information? Is this a criminal offence where evidence will need to be revealed as well as the whistleblower's identity?).

b) Is the whistleblower anxious about detriment? Has detrimental conduct already occurred or are they aware of any immediate threat?

c) Is the whistleblower involved in the wrongdoing or is it directed at them?

d) Does the report involve multiple types of wrongdoing?

e) How did the whistleblower obtain the information?

f) What is the whistleblower's relationship with the subject of the report?

g) What is the whistleblower's relationship with the organization?

Depending on the identified risks, organizations should identify and implement strategies and actions to prevent detriment against the whistleblower and other relevant interested parties, for example:

— protecting their identity;

— sharing information on a strictly need-to-know basis;

— providing support throughout the process, including regular communication, with special consideration and systems towards vulnerable people (e.g. children, young people, migrant workers, those with mental health issues or learning difficulties and older persons);

— changing workplace or reporting arrangements;

— warning subject(s) of the report or interested parties that detrimental conduct or breach of confidentiality can be a disciplinary offence.

The level of protection and related actions taken are dependent on the type and timing of whistleblowing and the potential consequences of wrongdoing(s) (e.g. on subject(s) of the report and other relevant interested parties).

Risks should be monitored and reviewed at various points in the process, such as when a decision is made to investigate, during the investigation into the report and once the outcome of an investigation is known, as well as, where appropriate, after the case has been closed.

8.4 Addressing reports of wrongdoing

8.4.1 Addressing the reported wrongdoing

Organizations should identify, implement, communicate and maintain a process that ensures investigations are conducted impartially by suitably qualified personnel. They should be fair and impartial to the business unit concerned, the whistleblower and the subject of the report.

Due process should be observed in any investigation arising out of a whistleblower report. For example, the investigation should be conducted without bias and the subject of the report of wrongdoing should be given the right to respond as required and given the option to be assisted.

In the interest of both the perception and reality of impartiality, consideration should be given as appropriate to employing outside investigators at arms' length from the organization, particularly where specialist investigative skills are not available internally or where the impartiality of an internal investigator is not ensured. To the extent possible, a multi-disciplinary approach should be taken where required. Professional investigation management includes but is not limited to the following principles.

a) Investigations should be adequately resourced.

b) Clear terms of reference and scope should be defined and documented.

c) The investigation process should be robust enough to withstand administrative, operational and legal review. An audit trail should be maintained relating investigation activities back to approved plans. The investigation should consider any subject of a report as being presumed innocent.

d) The investigation should not directly or indirectly interfere with a judicial investigation. It should cooperate where appropriate or required.

e) The investigation should secure and protect evidence.

f) The personal data should be managed in line with 7.5.4 (data protection).

g) The investigation should protect any information that could identify any subject of a report.

h) All investigations should be able to scale and adapt as the circumstances can change as the investigation progresses.

i) Communication should be clear and unambiguous, balancing the interests of organizations and the whistleblowers.

j) Organizations should communicate regularly, including at material progress steps, in the form of feedback to the whistleblower.

8.4.2 Protecting and supporting the whistleblower

Protection and practical support should be afforded to the whistleblower. Protection and support should begin as soon as a report of wrongdoing is received and continue throughout and following the reporting process. Responsibility should be clearly assigned within the organization for protection and support.

The organization should protect whistleblowers from detriment for reporting wrongdoing internally or externally to a relevant authority. Any policy should make clear that seeking to identify the whistleblower or detrimental conduct in connection with a whistleblower report is not tolerated and is a disciplinary matter.

Protection involves taking all reasonable steps to prevent detriment from occurring or contain identified detriment to prevent further harm. The strategies implemented will depend on the likely sources of harm identified through the assessment of risk (see 8.3.2).

Practical support involves encouraging and reassuring the whistleblower of the value of reporting wrongdoing and taking steps to assist their wellbeing. Support can be emotional, financial, legal or reputational.

Top management is accountable for ensuring support and protection. The whistleblowing management function (see 5.3.2) is responsible for ensuring that support and protection measures are implemented in the organization.

8.4.3 Addressing detrimental conduct

Whistleblowers can report detrimental conduct via the channels outlined in 8.2, as well as to the personnel responsible for supporting and protecting them.

If an organization becomes aware of, or suspects that a whistleblower is facing detrimental conduct, it should assess what action should be taken. Such assessment should take into account special consideration towards vulnerable people (e.g. children, young people, migrant workers, older persons).

If the detrimental conduct warrants investigation, this should be conducted by impartial personnel.

If it is established that detrimental conduct is occurring or has occurred, the organization should take reasonable steps to stop and address the detrimental conduct and support the whistleblower and other relevant interested parties.

Remediation can be needed. To the greatest extent possible, the whistleblower should be restored to a situation that would have been theirs had they not suffered detriment. For example:

a) reinstating the whistleblower in the same or equivalent position, with equal salary, responsibilities, working position and reputation;

b) fair access to promotion, training, opportunities, benefits, and entitlements;

c) restoration to the previous commercial position relative to the organization;

d) withdrawing litigation;

e) apologies given for any detriment suffered;

f) compensation for damage.

The organization should take appropriate disciplinary action against anyone found to be responsible for detrimental conduct.

8.4.4 Protecting the subject(s) of a report

Organizations should identify and implement strategies to protect the subject(s) of the report, for example:

a) protecting identity (to the extent possible);

b) conducting investigations in a manner that preserves confidentiality to the extent possible and appropriate to ensure that the subject(s) are not exposed to reputational harm (information is shared on a strictly need-to-know basis);

c) ensuring due process, including a timely, fair, impartial, confidential investigation and assistance;

d) providing support throughout the process, including regular communication;

e) if no evidence of wrongdoing was found, additional remedial measures can be considered, e.g. reputational, financial, employment status.

8.4.5 Protecting relevant interested parties

Relevant interested parties can include witnesses, others assisting or involved in a report of wrongdoing, internal investigators, family members, trade union representatives or others supporting the whistleblower, or those who are wrongly suspected of reporting wrongdoing. They should be protected from detriment, to the extent possible in the capacity, capability, and competence of the organization.

8.5 Concluding whistleblowing cases

Concluding a whistleblowing case designates the end of the processing of the report of wrongdoing.

A whistleblowing case will move into the concluding phase where no action is considered necessary in response to a report, where fact-finding determines no further investigation is warranted, where the report is referred to another process to be dealt with, or at the end of any investigation (whether or not wrongdoing is found).

Concluding whistleblowing cases can involve:

a) concluding an investigation, including issuing findings;

b) taking action in response to any recommendations (e.g. policy review, disciplinary actions);

c) communication to personnel responsible for supporting and protecting the whistleblower and other relevant interested parties;

d) identifying any ongoing protection measures;

e) collecting feedback from the whistleblower and other relevant interested parties;

f) identifying lessons learnt, as well as controls that need to be improved for policy, procedures or practices;

g) considering how, and in what form, a report of wrongdoing can be used for organizational learning as a case study;

h) retaining documented information (see 7.5) regarding concluding of the case, including date of closing, who approved closing and what action was taken.

Where wrongdoing is found, the organization should:

- take the appropriate measures to resolve the wrongdoing and to continuously monitor the effectiveness of those measures, in accordance with the appropriate organizational policies;
- administer appropriate sanctions;
- refer matters to the relevant authorities where appropriate and monitor the results or decisions made.

The organization may wish to consider how to acknowledge and give recognition to the whistleblower for reporting wrongdoing, with prior consent of the whistleblower (including, but not limited to, expressing gratitude and public commendation by top management).

The actions planned and taken, and any findings should be communicated in a timely manner to the whistleblower and relevant interested parties. This should include any independent avenues available to review the handling of the whistleblowing case.

Where there are legal restrictions on what can be communicated about the actions and findings (e.g. when the wrongdoing constitutes a criminal offence), the whistleblower should be notified of the reasons, where possible, of the limited communication.

NOTE It can be necessary to re-open a case where warranted.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The organization should determine:

- what needs to be monitored and measured;
- who is responsible for monitoring;
- the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
- when the monitoring and measuring should be performed;
- when the results from monitoring and measurement should be analysed and evaluated;
- to whom and how such information should be reported.

Documented information should be available as evidence of the results.

The organization should evaluate the performance and the effectiveness of the whistleblowing management system.

9.1.2 Indicators for evaluation

Organizations may consider how they can monitor and measure their whistleblowing management system performance by reference to several quantitative and qualitative indicators. The following is intended as a non-exhaustive list of examples of matters that can be monitored and measured by an organization in the context of its whistleblowing management system:

a) the number of reports of wrongdoing received by country, region and department;

b) the nature of the wrongdoing reported;

c) the time taken to acknowledge receipt of an initial report of wrongdoing;

d) for each step in the process, the time taken for completion;

e) the relative proportions over time of reports received via normal reporting lines, any internal alternative reporting systems and any external alternative reporting systems;

f) whistleblower feedback including satisfaction with the whistleblowing management system and suggestions for improvement;

g) periodic survey of personnel about awareness of and trust in the whistleblowing management system;

h) the proportion of reports that are sustained by an investigation against those that are not sustained;

i) the proportion of reports that fall outside of the scope of the whistleblowing management system;

j) the proportion of reports where the information provided was knowingly false;

k) the employment outcomes for whistleblowers (e.g. monitoring the proportion of whistleblowers who depart the organization after having made a report of wrongdoing and the reasons for their departure);

l) the proportion of reports resulting in corrective actions;

m) average time taken to investigate/close cases;

n) seriousness of issues raised;

o) the effectiveness and value of corrective actions taken.

An organization may compare its whistleblowing management system performance for each of its elements against a range of indicators in different reporting periods to aid continual improvement (see 10.2). When evaluating the indicators, careful consideration should be paid before arriving at conclusions (e.g. the numbers of reports received is not always a true reflection of the level of wrongdoing occurring; the absence of reports should lead to questions about the system's effectiveness).

9.1.3 Information sources

Information sources for the evaluation of the whistleblowing management system can include:

a) incoming reports;

b) investigation case files;

c) survey data;

d) feedback from whistleblowers and relevant interested parties such as subjects of the reports, witnesses, investigators, management, etc.;

e) indicator analysis;

f) other relevant available documentation.

Monitoring and measuring of performance is a continuous process which will vary depending on the organization and includes:

- qualitative assessment of the operation of the organization's whistleblowing management system;
- periodic quantitative assessment of performance indicators (in accordance with the examples set out in 9.1.1).

The process should maintain confidentiality.

9.2 Internal audit

9.2.1 General

The organization should conduct internal audits at planned intervals to provide information on whether the whistleblowing management system:

a) conforms to:

- the organization’s own requirements for its whistleblowing management system;
- the recommendations of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization should 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 should consider the importance of the processes concerned and the results of previous audits.

The organization should:

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;

d) ensure that the results of the audit are considered and acted upon as appropriate.

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

9.3 Management review

9.3.1 General

Top management should review the organization’s whistleblowing management system and report its findings to the governing body, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review should include:

a) the status of actions from previous management reviews;

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

c) changes in needs and expectations of interested parties that are relevant to the whistleblowing management system;

d) information on the whistleblowing management system performance, including trends in:

- nonconformities and corrective actions;

- monitoring and measurement results;
- audit results;

e) opportunities for continual improvement and learning;

9.3.3 Management review results

The results of the management review should include decisions related to continual improvement opportunities and any need for changes to the whistleblowing management system.

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

10 Improvement

10.1 Continual improvement

The organization should continually improve the suitability, adequacy and effectiveness of the whistleblowing management system. When an organization determines that there is a need for change to the whistleblowing management system, such change should be carried out in a planned manner (see 6.3) and should include consideration of the following:

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

b) the integrity of the whistleblowing management system;

c) the availability of resources;

d) the allocation or reallocation of responsibilities and authority;

e) the rate, extent and time frame of implementing the changes;

f) the scope of the whistleblowing management system.

10.2 Nonconformity and corrective action

When a nonconformity with the whistleblowing management system occurs, the organization should:

a) react to the nonconformity and, as applicable:

- take action to control and correct it;
- 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:

- reviewing the nonconformity;
- determining the causes of the nonconformity;
- determining if similar nonconformities exist, or can potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the whistleblowing management system, if necessary.

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

Documented information should be available as evidence of:

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

Bibliography

[1] ISO 19011, *Guidelines for auditing management systems*

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

[3] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[4] ISO 31000, *Risk management — Guidelines*

[5] ISO 37001:2016, *Anti-bribery management systems — Requirements with guidance for use*

[6] ISO 37301, *Compliance management systems — Requirements with guidance for use*

[7] ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*

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

ICS 03.100.02; 03.100.01; 03.100.70

Price based on 33 pages