



# SLOVENSKI STANDARD SIST ISO 37002:2021

01-december-2021

---

## Sistem vodenja prijavljanja nepravilnosti - Smernice

Whistleblowing management systems - Guidelines

Systèmes de management des alertes - Lignes directrices

Ta slovenski standard je istoveten z: **ISO 37002:2021**

[SIST ISO 37002:2021](https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021)

<https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021>

### **ICS:**

03.100.01	Organizacija in vodenje podjetja na splošno	Company organization and management in general
03.100.02	Upravljanje in etika	Governance and ethics
03.100.70	Sistemi vodenja	Management systems

**SIST ISO 37002:2021**

**en,fr**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO 37002:2021](#)

<https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021>

INTERNATIONAL  
STANDARD

ISO  
37002

First edition  
2021-07

---

---

**Whistleblowing management  
systems — Guidelines**

*Systèmes de management des alertes — Lignes directrices*

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO 37002:2021](https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021)

<https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021>



Reference number  
ISO 37002:2021(E)

© ISO 2021

## iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST ISO 37002:2021

<https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021>



### **COPYRIGHT PROTECTED DOCUMENT**

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Context of the organization</b> .....	<b>7</b>
4.1 Understanding the organization and its context.....	7
4.2 Understanding the needs and expectations of interested parties.....	8
4.3 Determining the scope of the whistleblowing management system.....	8
4.4 Whistleblowing management system.....	9
<b>5 Leadership</b> .....	<b>9</b>
5.1 Leadership and commitment.....	9
5.1.1 Governing body.....	9
5.1.2 Top management.....	10
5.2 Whistleblowing policy.....	10
5.3 Roles, responsibilities and authorities.....	11
5.3.1 Top management and governing body.....	11
5.3.2 Whistleblowing management function.....	12
5.3.3 Delegated decision-making.....	12
<b>6 Planning</b> .....	<b>13</b>
6.1 Actions to address risks and opportunities.....	13
6.2 Whistleblowing management system objectives and planning to achieve them.....	13
6.3 Planning of changes.....	14
<b>7 Support</b> .....	<b>14</b>
7.1 Resources.....	14
7.2 Competence.....	14
7.3 Awareness.....	15
7.3.1 General.....	15
7.3.2 Personnel training and awareness measures.....	15
7.3.3 Training for leaders and other specific roles.....	16
7.4 Communication.....	17
7.5 Documented information.....	18
7.5.1 General.....	18
7.5.2 Creating and updating documented information.....	18
7.5.3 Control of documented information.....	18
7.5.4 Data protection.....	19
7.5.5 Confidentiality.....	19
<b>8 Operation</b> .....	<b>20</b>
8.1 Operational planning and control.....	20
8.2 Receiving reports of wrongdoing.....	22
8.3 Assessing reports of wrongdoing.....	23
8.3.1 Assessing the reported wrongdoing.....	23
8.3.2 Assessing and preventing risks of detrimental conduct.....	24
8.4 Addressing reports of wrongdoing.....	25
8.4.1 Addressing the reported wrongdoing.....	25
8.4.2 Protecting and supporting the whistleblower.....	26
8.4.3 Addressing detrimental conduct.....	26
8.4.4 Protecting the subject(s) of a report.....	27
8.4.5 Protecting relevant interested parties.....	27
8.5 Concluding whistleblowing cases.....	27
<b>9 Performance evaluation</b> .....	<b>28</b>

**ISO 37002:2021(E)**

9.1	Monitoring, measurement, analysis and evaluation.....	28
9.1.1	General.....	28
9.1.2	Indicators for evaluation.....	28
9.1.3	Information sources.....	29
9.2	Internal audit.....	30
9.2.1	General.....	30
9.2.2	Internal audit programme.....	30
9.3	Management review.....	30
9.3.1	General.....	30
9.3.2	Management review inputs.....	30
9.3.3	Management review results.....	31
<b>10</b>	<b>Improvement.....</b>	<b>31</b>
10.1	Continual improvement.....	31
10.2	Nonconformity and corrective action.....	31
	<b>Bibliography.....</b>	<b>33</b>

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST ISO 37002:2021](https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021)

<https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021>

## 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](http://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](http://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](http://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](http://www.iso.org/members.html).

## ISO 37002:2021(E)

### 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.



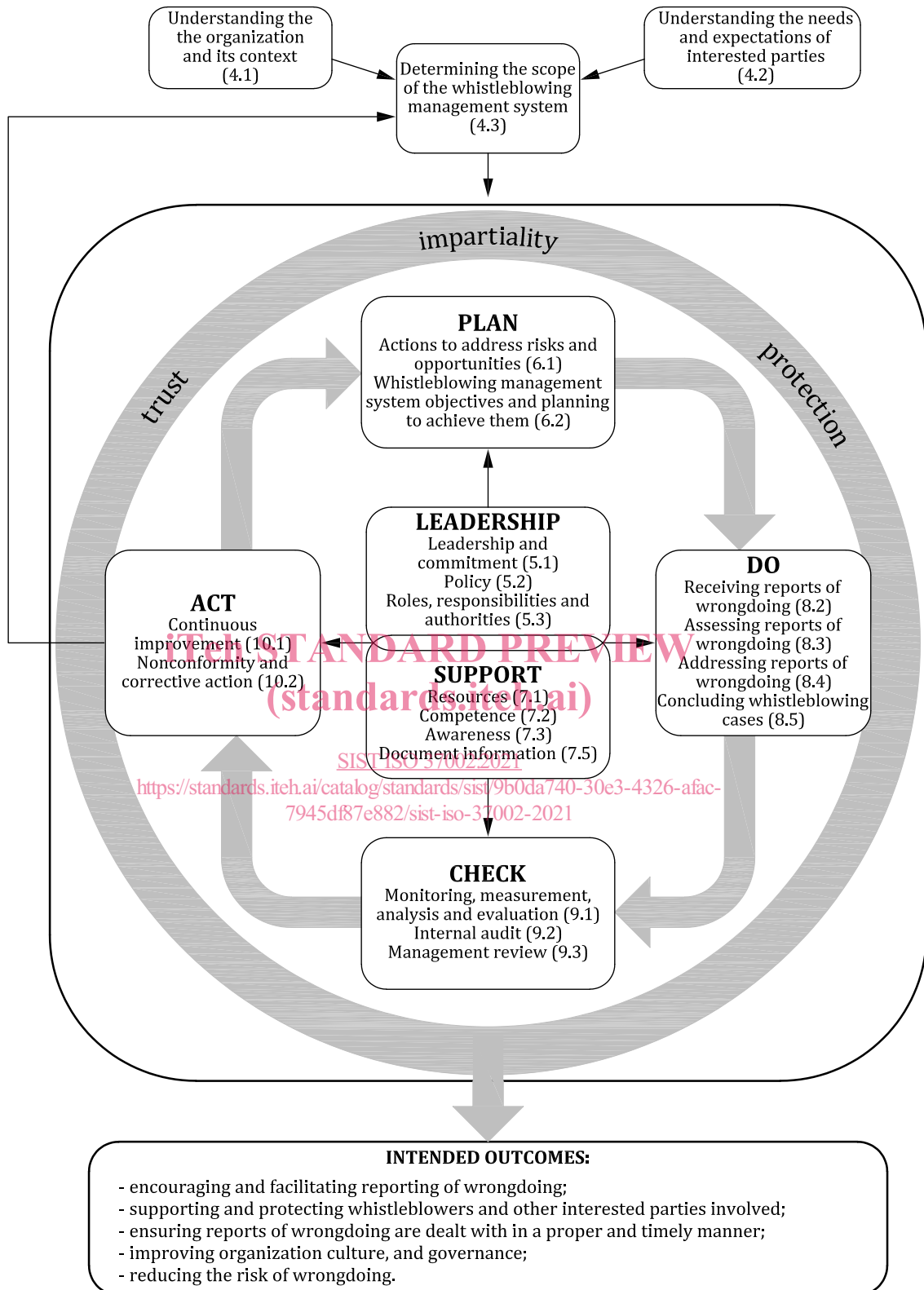


Figure 1 — Overview of a whistleblowing management system

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO 37002:2021](#)

<https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021>

# 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.

iTeh STANDARD PREVIEW

## 2 Normative references (standards.iteh.ai)

There are no normative references in [this document](#).

<https://standards.iteh.ai/catalog/standards/sist/9b0da740-30e3-4326-afac-7945df87e882/sist-iso-37002-2021>

## 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.

## ISO 37002:2021(E)

### 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.