International

ISO 37003

Fraud control management systems — Guidance for organizations managing the risk of fraud

Systèmes de management du contrôle de la fraude — Lignes directrices destinées aux organisations gérant le risque de fraude

First edition
2025-05

Reference number
ISO 37003:2025(en)

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

Licensing and use terms

As stated above, ISO documents, as well as any updates and/or corrections, and any intellectual property or other rights pertaining thereto, are owned by ISO. ISO documents are licensed, not sold. This document does not in any way operate to assign or transfer any intellectual property rights from ISO to the user. ISO documents are protected by copyright law, database law, trademark law, unfair competition law, trade secrecy law, and any other applicable law. Users acknowledge and agree to respect ISO's intellectual property rights in the ISO documents.

The use of ISO documents is subject to the terms and conditions of the applicable licence agreement.

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

a) Licence Type:

   1) Single registered end-user licence (watermarked in the user's name) for the specified Purpose. Under this license, the user cannot share the ISO document with a third party, including on a network.

   2) Network licence for the specified Purpose. The network licence can be assigned to either unnamed concurrent end-users or named concurrent end-users within the same organization.

b) Purpose:

1) Internal Purpose. Internal use only within the user's organization, including but not limited to own implementation ("Internal Purpose").

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

2) External Purpose. External use, including but not limited to:

— testing services;

— inspection services;

— certification services;

— auditing services;

— consulting services;

— conformity assessment scheme development and implementation;

— training services;

— education;

— research;

— software development and other digital platform or software-enabled digital services;

— any other services or activities conducted by the user or the user's organization to third parties, whether for commercial or non-commercial purposes ("External Purpose").

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

Unless users have been granted use rights according to the above provisions, they are not granted the right to share or sublicense ISO documents inside or outside their organization for either Purpose. If users wish to obtain additional use rights for ISO documents or their content, users can contact ISO or the ISO member body in their country to explore possible options.

If the user or the user's organization is granted a licence for the External Purpose of providing any of the following services to third parties:

— testing services;

— inspection services;

certification services;

— auditing services;

— consulting services,

and if any of these five (5) services reference, rely upon, incorporate, or otherwise make use of any aspect, requirement, provision, or any other information of any ISO document, the user or the user's organization agrees to verify that the third party receiving such services has obtained from the ISO member body in their country, any other ISO member body, ISO or an authorized third-party distributor, a valid licence for its own implementation of such ISO document or other use related to such services. This verification obligation must be included in the applicable licence agreement obtained by the user or the user's organization.

ISO documents must not be disclosed to third parties, and users must use them solely for the purpose specified in the purchase order and/or applicable licensing agreement. Unauthorized disclosure or use of ISO documents beyond the licensed purpose is prohibited and can result in legal action.

Use restrictions

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

— use ISO documents for any purpose other than the Purpose;

— grant use or access rights to ISO documents beyond the Licence Type;

— disclose ISO documents beyond the intended Purpose and/or Licence Type;

— sell, lend, lease, reproduce, distribute, import/export or otherwise commercially exploit ISO documents. In the case of documents that are joint publications (such as ISO/IEC documents), this clause applies to the respective joint copyright ownership;

— assign or otherwise transfer ownership of ISO documents, in whole or in part, to any third party.

Regardless of the Licence Type or Purpose for which users are granted access and use rights for ISO documents, users are not permitted to access or use any ISO documents, in whole or in part, for any machine learning and/or artificial intelligence and/or similar purposes, including but not limited to accessing or using them

a) as training data for large language or similar models, or

b) for prompting or otherwise enabling artificial intelligence or similar tools to generate responses.

Such use is only permitted if expressly authorized through a specific licence agreement by the ISO member body in the requester's country, another ISO member body, or ISO. Requests for such authorization are considered on a case-by-case basis to ensure compliance with intellectual property rights. Specifically, it is not possible to claim the benefit of copyright exception of Article 4 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, for the purpose of text and data mining on ISO documents, as ISO hereby opts out of this exception.

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

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

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

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

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

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

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

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 http://www.iso.org/members.html.

Fraud is a risk for all organizations in the private, public or not-for-profit sectors. Fraud events can significantly impact the financial position of the target organization and often have flow-on financial consequences for global and local economies. Fraud can lead to serious legal and financial consequences as well as enduring psychological and emotional harm for the individuals involved. For a summary of the types of fraud commonly encountered by organizations, see Annex A.

The pervasiveness and increasing sophistication of information technology, the rapid uptake of electronic payment systems by the general population and economic globalization have led to an increased incidence of external fraudulent attack on organizations across all sectors.

Managing and controlling the risk of fraud should be considered by the leadership of all organizations.

NOTE For more information on fraud as it relates to governance, see ISO 37000:2021, 6.9.

This document includes guidance on:

a) creating and maintaining processes for fraud risk identification, assessment and monitoring;

b) mitigating internal and external fraud, including fraud against, and by, the organization;

c) detecting fraud against or by the organization based on its assessed fraud risk exposures;

d) effective response to fraud events in order to ensure that:

   — damage to the organization's image can be minimized;

   — its reputation can be restored and improved;

   — funds lost due to fraud can be recovered.

e) ensuring continual improvement.

Following this guidance cannot provide assurance that fraud has not occurred or will not occur in the future as it is not possible to eliminate the risk of fraud. However, it will help organizations to effectively manage fraud risk and to respond appropriately to fraud events and avoid or reduce the compliance liability risk of the organization.

Effective fraud control requires the organization to commit to prevention, detection and response initiatives underpinned by leadership, planning and resourcing as summarised in Figure 1.

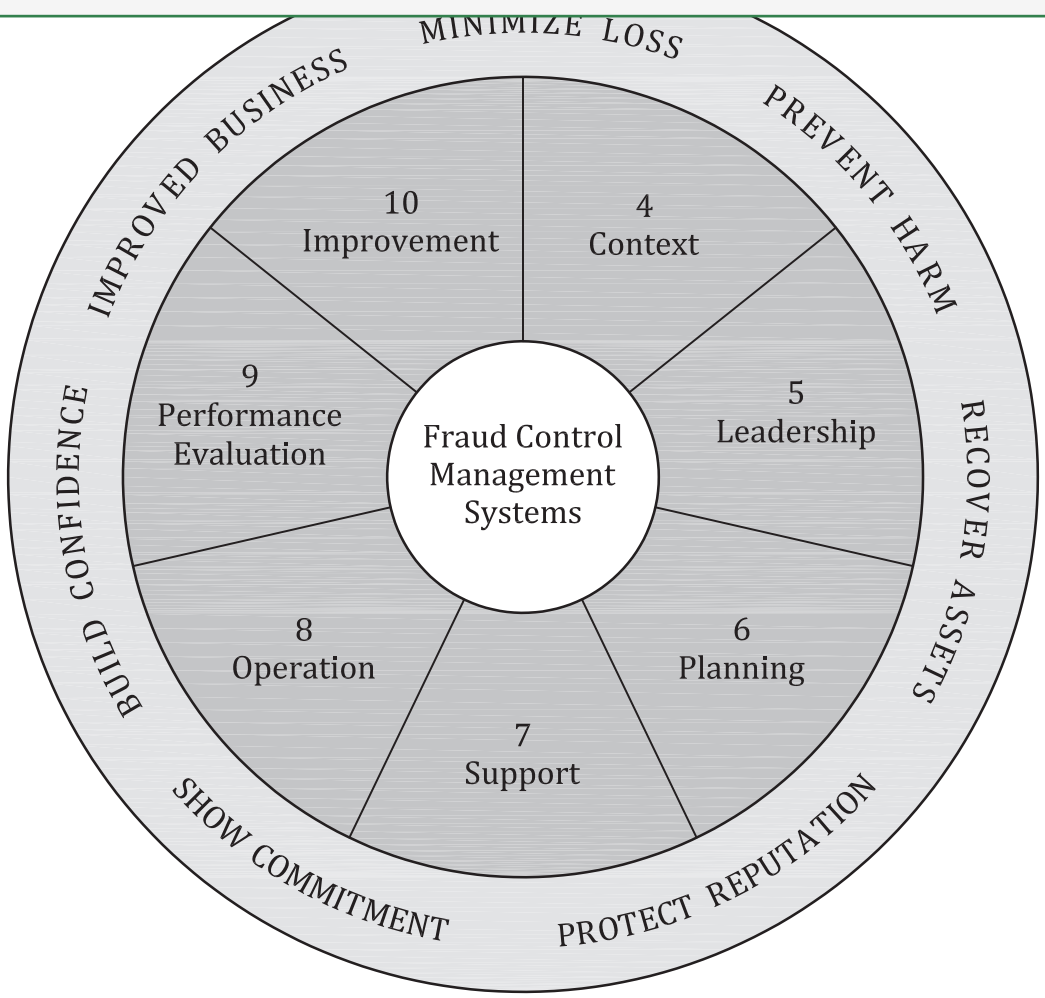

Figure 1 — Principles, structure and objectives of this document