~~organ~~ ISO~~-~~/FDIS 37003

ISO~~-~~/TC~~-~~ 309~~ /WG 8~~

Secretariat: BSI

Date: 2025-01-17

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

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

~~© ISO 2024~~

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

FDIS stage

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

Published in Switzerland

Contents

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO 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 ~~www.iso.org/patents.~~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~~www.iso.org/iso/foreword.html.

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

~~A list of all parts in the ISO 37000 series can be found on the ISO website~~*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.

Introduction

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. ~~It~~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.~~ Annex A.

The pervasiveness and increasing sophistication of information technology, the rapid ~~take-up~~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:~~ 2022, clause~~2021, 6.9~~ – Risk Governance~~.

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;

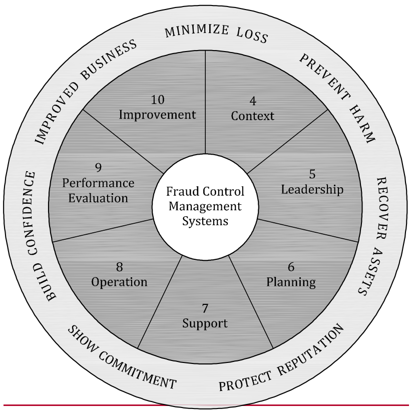
d) effective response to fraud events in order to ensure that:

- — 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 ~~occur~~ as it is not possible to eliminate the risk of fraud~~; however.~~. 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.



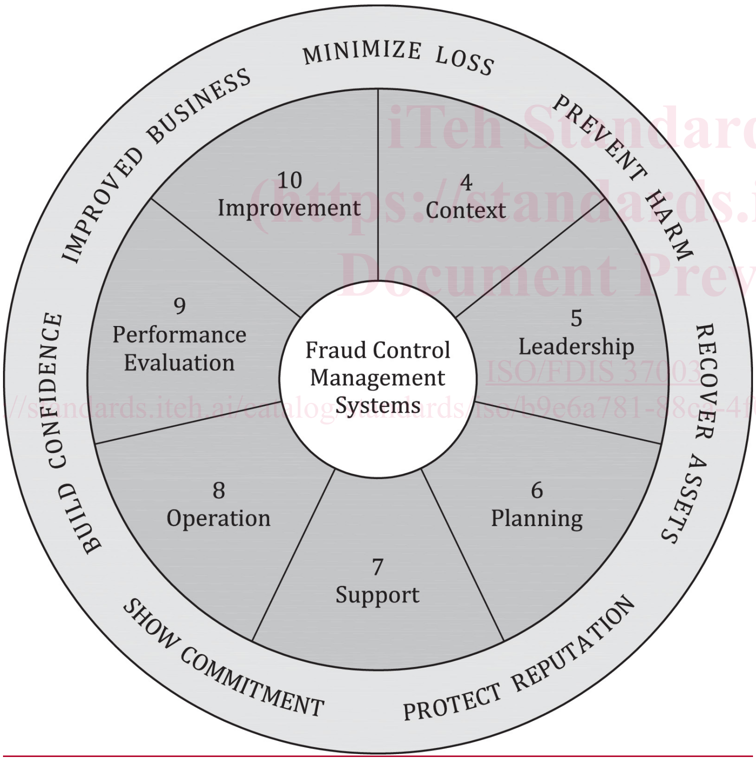


Figure 1 — Principles, structure and objectives of ~~ISO 37003~~ this document

Fraud ~~Control Management Systems —~~ control management systems — Guidance for organizations managing the risk of fraud

1 Scope

This document provides guidance for organizations for the development, implementation and maintenance of an effective fraud control management system (FCMS~~), including~~). This includes fraud prevention, early detection of fraud and effective response to fraud events that have occurred or can occur in the future.

The document provides guidance for managing the risk of fraud, including:

a) internal fraud against the organization;

b) external fraud against the organization;

c) internal fraud in collaboration with business associates or other third parties;

d) external fraud in collaboration with the organization’s personnel;

e) fraud by the organization or by persons purporting to act on behalf of and in the interests of the organization.

This document is applicable to all organizations, regardless of type, size, nature of activity~~,~~ and whether in the public or private, profit or not-for-profit sectors. It is not intended to assist consumers in preventing, detecting or responding to what is generally termed ~~‘~~"consumer ~~fraud’.~~ fraud".

~~3~~2 Normative references

There are no normative references in this document.

~~5~~3 Terms and definitions

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

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

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

Field Code Changed

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

Field Code Changed

~~5.1~~3.1~~3.1~~

fraud

intentional dishonest act causing actual or potential gain or loss that creates social or economic harm

Note~~–~~ 1~~–~~ to entry:~~–~~ Fraud also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal financial benefit.

Note~~-~~ 2~~-~~ to entry:~~-~~ Fraudulent conduct need not necessarily represent a breach of law.

Note 3 to entry: Fraud can involve fraudulent conduct by internal and/or external parties targeting the *organization* ~~(3.3)~~(3.3) or fraudulent conduct by the organization itself targeting external parties.

Note 4 to entry: Fraud can include loss of moneys or other property by persons internal and external to the organization and where deception is used at the time, immediately before or immediately following the activity.

Note 5 to entry: Fraud can be external or internal or both. External fraud is where no perpetrator is employed by or has a close association with the target organization. Internal fraud is where at least one perpetrator is employed by or has a close association with the target organization and has detailed internal knowledge of the organization's operations, systems and procedures.

~~5.2~~3.2

~~3.2~~

fraud event

instance of *fraud* ~~(3.1)~~(3.1) against or by an *organization* ~~(3.3)~~(3.3)

~~5.3~~3.3~~3.3~~

organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* ~~(3.15)~~(3.14)

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 *fraud* ~~*control management system (3.11).*~~*controlmanagement system* (3.11).

~~5.4~~3.4~~3.4~~

target organization

organization ~~(3.3)~~(3.3) that is the object of a *fraud event* ~~(3.2).~~ (3.2).

~~5.5~~3.5~~3.5~~

interested party

person or *organization* ~~(3.3)~~(3.3) that can affect, be affected by, or perceive itself to be affected by a decision or activity

~~5.6~~3.6~~3.6~~

top management

person or group of people who directs and controls an *organization* ~~(3.3)~~(3.3) 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* ~~(3.10)~~(3.10) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

Note 3 to entry: Organizations can be organized depending on which legal framework they are obliged to operate
under and also according to their size, sector, etc. Some organizations have both a *governing body* ~~(3.7)~~(3.7) and *top*
management ~~(3.6),~~(3.6), while some organizations do not have responsibilities divided into several bodies. These
variations, both in respect of organization and responsibilities, can be considered when applying the requirements in Clause 5.

~~in Clause 5.~~

~~5.8~~3.7 ~~3.7~~

governing body

person or group of people who have ultimate accountability for the whole *organization* ~~(3.3)~~(3.3)

Note 1 to entry: A governing body can be explicitly established in a number of formats including, but not limited to, a board of directors, supervisory board, sole director, joint and several directors, or trustees.

Note 2 to entry: ISO management system standards make reference to the term “top management” to describe a role that, depending on the standard and organizational context, reports to, and is held accountable by, the governing body.

Note 3 to entry: Not all organizations, particularly small and medium organizations, will have a governing body separate from top management. In such cases, top management exercises the role of the governing body.

[SOURCE: ISO 37000:2021, 3.3.4, ~~notes to entry modified]~~modified — The Notes to entry were reordered: Note 2 to entry is now Note 1 to entry; Note 3 to entry is now Note 2 to entry; and Note 3 to entry was added.]

~~5.10~~3.8 ~~3.8~~

personnel

organization’s ~~(3.3)~~(3.3) directors, officers, employees, temporary staff or workers, and volunteers

Note 1 to entry: Different types of personnel pose different types and degrees of fraud *risk* ~~(3.16)~~(3.15) and can be treated differently by the organization's fraud risk assessment and fraud risk management procedures.

[SOURCE: ISO ~~DIS~~ 37001:~~2024~~20—[1], 3.24, modified ~~–~~— Note 1 has been amended and Note 2 to entry has been deleted]

~~5.11~~3.9 ~~3.9~~

business associate

external party with whom the *organization* ~~(3.3)~~(3.3) has, or plans to establish, some form of business relationship

Note 1 to entry: Business associate includes but is not limited to clients, customers, joint ventures, joint venture partners, consortium partners, outsourcing providers, contractors, consultants, sub-contractors, suppliers, vendors, advisors, agents, distributors, representatives, intermediaries and investors. This definition is deliberately broad and should be interpreted in line with the fraud *risk* ~~(3.16)~~(3.15) profile of the organization to apply to business associates which can reasonably expose the organization to fraud risks.

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

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

[SOURCE: ISO 37001:~~2024,~~20—, 3.26, modified]

~~5.12~~3.10 ~~3.10~~

management system

set of interrelated or interacting elements of an *organization* ~~*(3.3)*~~(3.3) to establish *policies* ~~*(3.12)*~~(3.12) and *objectives* ~~*(3.15)*~~(3.14) as well as *processes* ~~*(3.20)*~~(3.18) to achieve those objectives

[1] Under preparation. Stage at the time of publication: ISO/PRF 37001:2025.

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.

3.11 ~~3.11~~

fraud control management system (FCMS)

part of the overall *management system* ~~(3.10)~~(3.10) for controlling the risks of *fraud* ~~(3.1)~~(3.1) against or by an *organization* ~~(3.3)~~(3.3)

~~5.13~~3.12 ~~3.12~~

policy

intentions and direction of an *organization* ~~(3.3)~~(3.3) as formally expressed by its *top management* ~~(3.6)~~(3.6)

~~5.15~~3.13 ~~3.14~~

conflict of interest

situation in which an interested party has personal interest or organizational interest, directly or indirectly, that ~~could~~can compromise, or interfere with, the ability to act impartially in carrying out their duties in the best interest of the *organization* ~~(3.3)~~(3.3)

Note 1 to entry: There ~~could~~can be different types of personal interests: business, financial, family, professional, religious or political.

Note 2 to entry: Organizational interest relates to the interests of an organization or part of an organization (e.g. team or department) rather than an individual.

[SOURCE: ISO ~~DIS~~ 37009:~~2024~~20—[2], 3.1.10]

~~5.17~~3.14 ~~3.15~~

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 or *process* ~~(3.20).~~ (3.18).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as a fraud control 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 *fraud* ~~*control management*~~*controlmanagement* *systems* ~~(3.11),~~(3.11), fraud control objectives are set by the *organization* ~~(3.3),~~(3.3), consistent with the fraud control *policy* ~~(3.12),~~(3.12), to achieve specific results.

~~5.18~~3.15 ~~3.16~~

risk

effect of uncertainty on *objectives* ~~(3.15)~~(3.14)

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

[2] Under preparation. Stage at the time of publication: ISO/DIS 37009:2024.