SLOVENSKI STANDARD
oSIST ISO/DIS 37003:2024

01-marec-2024

Sistemi vodenja nadzora nad goljufijami - Napotki za organizacije, ki se odzivajo na tveganje goljufij

Fraud Control Management Systems - Guidance for organizations responding to the risk of fraud

Systèmes de management du contrôle de la fraude — Recommandations aux organisations en réponse aux risques de fraude

Ta slovenski standard je istoveten z: **ISO/DIS 37003**

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

oSIST ISO/DIS 37003:2024 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 37003

ISO/TC **309**

Secretariat: **BSI**

Voting begins on:
2024-01-15

Voting terminates on:
2024-04-08

Fraud Control Management Systems — Guidance for organizations managing the risk of fraud

ICS: 03.100.02; 03.100.70; 03.100.01

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 37003:2024(E)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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

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

Fraud is a risk for all organizations including private, public and 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 can lead to serious legal and financial consequences as well as enduring psychological and emotional harm for the individuals involved. For a summary of types of fraud commonly encountered by commercial organizations see Annex A.

The pervasiveness and increasing sophistication of information technology, the rapid take-up 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 is a core governance issue which should be considered by the leadership of all organizations, including the governing body and top management.

This document includes guidance on:

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

(b) mitigating of 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 exposure;

(d) effective response to fraud events such that lessons are learned that can be applied to the mitigation framework, 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.

Following this guidance cannot provide assurance that fraud has not occurred or will not in the future occur as it is not possible to eliminate the risk of fraud; however, it will help organizations to effectively manage fraud risk and 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 prevent, detect and response initiatives underpinned by leadership, planning and resourcing as summarised in Figure 1.

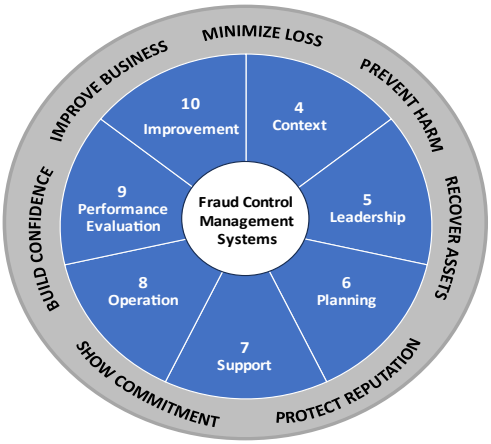

Figure 1 — Principles, structure and objectives of ISO 37003

Fraud 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 fraud prevention, early detection of fraud and effective response to fraud events that have occurred or may occur in the future.

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

(i) internal fraud against the organization;

(ii) external fraud against the organization;

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

(iv) external fraud in collaboration with the organization's personnel;

(v) 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'.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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) or fraudulent conduct by the organization itself targeting external parties.

Note 4 to entry: Fraud can include theft 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.

3.2
fraud event
instance of *fraud* (3.1) against or by an *organization* (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)

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).*

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

3.4
target organization
organization (3.3) that is the object of a *fraud event* (3.2).

3.5
interested party
person or *organization* (3.3) that can affect, be affected by, or perceive itself to be affected by a decision or activity

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

3.6
top management
person or group of people who directs and controls an *organization* (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) 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.

3.7
governing body
person or group of people who have ultimate accountability for the whole *organization* (3.3)

Note 1 to entry: *Top management* (3.6) reports to and is held accountable by governing body.

Note 2 to entry: Not all organizations, particularly small organizations, will have a governing body separate from top management.

Note 3 to entry: A governing body can include, but is not limited to, board of directors, committees of the board, supervisory board, trustees or overseers.

[SOURCE: ISO 37000:2021, 3.3.4, notes to entry modified]

3.8
personnel
organization's directors, officers, employees, temporary staff or workers, and volunteers

[SOURCE: ISO 37000:2021, 3.3.6]

3.9
business associate
external party with whom the organization 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 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 bribery 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 37001:2016, 3.26, modified]

3.10
management system
set of interrelated or interacting elements of an *organization (3.3)* to establish *policies (3.12)* and *objectives (3.15)* as well as *processes (3.20)* 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.

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

3.12
policy
intentions and direction of an *organization* (3.3) as formally expressed by its *top management (3.6)*

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

3.13
code of behaviour
documented information (3.23) setting out the applicable standards of behaviour and conduct

3.14
conflict of interest
situation where business, financial, family, political or personal interests could interfere with the judgment of persons in carrying out their duties for the *organization* (3.3)

[SOURCE: ISO 37001:2016, 3.29]

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).

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 systems* (3.11), fraud control objectives are set by the *organization* (3.3), consistent with the fraud control *policy* (3.12), 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.

3.16
risk
effect of uncertainty on *objectives* (3.15)

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.

3.17
level of risk
magnitude of a *risk* (3.16) or combination of risks, expressed in terms of the combination of consequences and their likelihood

[SOURCE: ISO 37000:2021, 3.1.10]

3.18
risk assessment
overall process of risk identification, risk analysis and risk evaluation

[SOURCE: ISO 31073:2022, 3.3.8]

3.19
control
measure that maintains and/or modifies *risk* (3.16)

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31000:2018, 3.8]

3.20
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

