Technical note on
ISO 37003
Fraud Control Management Systems

1 Executive summary
General overview

ISO 37003 was published on the 29th of May, 2025, aiming at strengthening organisational resilience against fraud risk

Context

- The **growing complexity** of technology, widespread use of electronic payment systems, and the effects of economic globalisation have contributed to a **rise in external fraud attempts targeting organisations across all sectors.** These evolving threats **demand more robust and proactive approaches to risk management.** As a result, the **effective governance of fraud risk has become a strategic priority**, requiring active oversight and commitment from senior leadership to safeguard organisational integrity, financial stability, and stakeholder trust.
- In response to these challenges, the final version of **ISO 37003** has been published to provide a **structured** and **comprehensive framework** for **managing fraud risk.**

Objective

- **Helping organisations to prevent, detect, and respond to both internal and external fraud in a systematic and consistent manner,** thereby strengthening resilience and promoting a culture of integrity.

Main contents: this ISO provides guidance on...

- **Creation** and **maintenance** of **processes** for the **identification, evaluation,** and **monitoring** of **fraud** risks

- **Mitigation of internal and external fraud**, including fraud against and by the organization

- **Detecting fraud** against or by the organization **based on its exposure** evaluated to the **risk** of fraud

- **Effective response** to **fraud** cases, so that lessons can be drawn and applied to the mitigation framework, to ensure that:
  - **damage** to the **organization's image** is **minimized**
  - its **reputation** can be restored and **improved**
  - lost **funds** can be **recovered** due to fraud

What does ISO consider as Fraud?

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

- **Falsification**, **concealment**, **destruction** or **use of falsified documents** for business purposes, or misuse of information or position for personal gain.
- May not constitute a **breach of law**.
- May involve **internal/external parties** targeting the organization, or the organization targeting others.
- **Loss of money** or **property** through deception before, during, or after the act.
- May be **external** (no link to the organization) or **internal** (perpetrator has insider knowledge).

ManagementSolutions
Making things happen

ISO 37003 provides comprehensive coverage for the management of fraud risk (internal and external) in organizations, considering the standard ISO structure and the main areas of management to be covered

Scope

The scope to cover fraud is comprehensive, considering both internal and external fraud

- Internal fraud against the organization

- External fraud against the organization

- Internal fraud in collaboration with business partners or other third parties

- External fraud in collaboration with the organization's personnel

- Fraud by the organization or individuals pretending to act on its behalf or in its interest

Structure*

The standard is structured into the 10 typical ISO blocks, from organizational context to continuous improvement
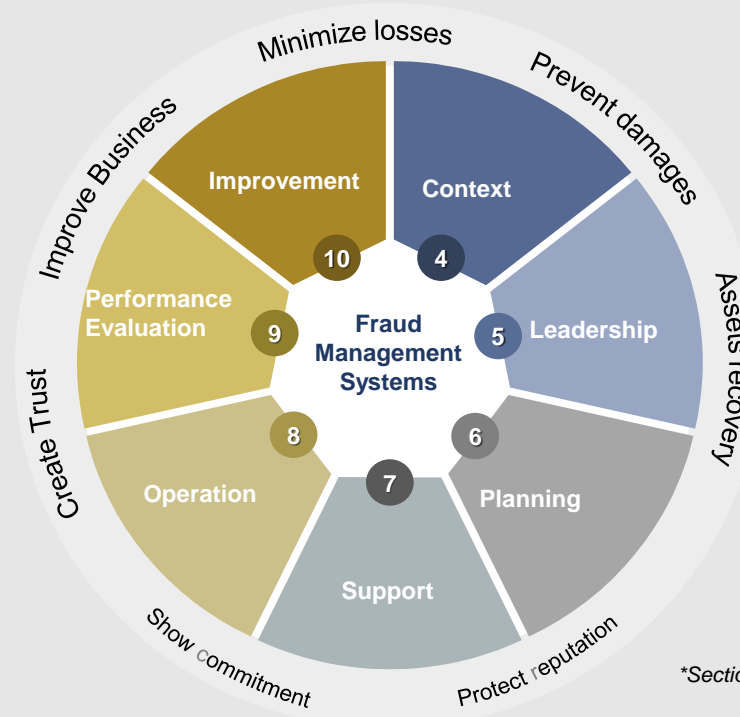
*Sections 1 to 3 have not been incorporated into the diagram, as they are introductory and related to scope, regulations, and definitions.

Relevant blocks

The main fraud risk management areas are aligned with other ICT standards such as NIST

- Foundations for fraud control

- Prevention

- Detection

- Response

Management Solutions has extensive experience in fraud management projects, as well as solid capabilities to help achieve practical results in an agile manner

Proven experience in fraud risk governance projects	• **Multiple collaborations in Fraud Management projects** (Europe + America) in large corporations (financial and insurance entities, banks, energy, other sectors), including the **coordination and leadership of global fraud management programs**, from defining the strategy and the pain points to mitigate, to the securitization of processes, considering operational and technological antifraud models:
	  i. Definition and evolution of fraud management frameworks (policies, standards and procedures)
	  ii. Evolution of fraud functions in the organization, including roles and responsibilities, Governance, committee structure and relationship model
	  iii. Support in the constitution, coordination and development of support material and reporting model to Senior Management, including the development of KPI Framework and Dashboards
	  iv. Definition of training and awareness programs, for both internal and external employees
	  v. Development and implementation of fraud risk mitigation methodologies, with an E2E process vision
	  vi. Definition of specific control frameworks to ensure optimal mitigation of operational fraud risk in digital processes, credit admission, internal fraud processes, physical channels, etc.

Experts in the development of advanced analytics models	• Development of **modeling projects** of various types in **diverse sectors and industries**, and with various work schemes and methodologies, from the definition and evolution of **MRM, Data Governance and Data Quality Frameworks**, to the development, optimization, calibration and validation of models (supervised and unsupervised), using best practices
High-value profiles with expertise in Fraud, IT Risk and Data Security	• Professionals with strong **comprehension, communication, challenge/advisory capabilities of high value, expertise in Fraud, IT Risk and Data Security, and their relationship with risk management, processes and cybersecurity (Cross vision)** • **Extensive knowledge of regulation, standards and market best practices in Fraud and IT Risk management** • Understanding of **business processes**, knowledge of **risk management methodologies** and **analytical capabilities**
Experts in Fraud Risk Management tools	• Extensive knowledge of tools that constitute the **fraud management and monitoring tools ecosystem**, from the fraud **backend (antifraud engine),** to **satellite tools** that provide **additional information and security inputs** (digital and device information, contact information, behavior, volume monitoring, customer identity, ...)

Management Solutions
Making things happen

International
One Firm

Multiscope
Team

Best practice
know-how

Proven
Experience

Maximum
Commitment

Iñigo Soroa Echevarría
Partner at Management Solutions
Inigo.soroa@msnorthamerica.com

Juan Manuel López Medina
Manager at Management Solutions
juan.manuel.lopez@msspain.com

Marta Hierro
Partner at Management Solutions
Marta.Hierro@msspain.com

For more information please visit

www.managementsolutions.com

Or follow us at: in X f ⓘ ▶