INTERNATIONAL STANDARD

ISO 4669-1

First edition
2023-05

Document management — Information classification, marking and handling —

Part 1: Requirements

Gestion des documents — Traitement, marquage et classification de l'information —

Partie 1: Exigences

Reference number
ISO 4669-1:2023(E)

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

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Principles 3
5 ICMH system design 4
5.1 Classification scheme design 4
5.1.1 Classification criteria 4
5.1.2 Hierarchy 5
5.1.3 Classification scheme equivalence 6
5.1.4 Information asset life cycle 6
5.1.5 Default classifications 7
5.1.6 Information assets that are not marked 8
5.1.7 Descriptors and dependencies 8
5.2 Marking scheme design 9
5.2.1 Marking design criteria 9
5.2.2 Placement and style of marking 9
5.3 Handling scheme design 10
5.3.1 Handling design criteria 10
5.3.2 Information handling during creation and capture 10
5.3.3 Information re-use in other information assets 11
5.3.4 Editing and changes to an information asset 11
5.3.5 Information aggregation 11
5.3.6 Access to and handling of information 11
5.3.7 Information storage 12
5.3.8 Information replication and rendering 12
5.3.9 Information redaction 13
5.3.10 Information distribution, sharing and exchange 13
5.3.11 Information archiving and disposal 14
5.3.12 Information security 15
5.4 ICMH system evaluation 15
5.4.1 Evaluation programme 15
5.4.2 Monitoring and testing 15
5.4.3 Auditing and assurance 16
5.4.4 Measurement 16
5.4.5 Incident management and investigation 16
5.4.6 Reporting and lesson learning 16
6 ICMH system revision 16
6.1 Scheme revision 16
6.2 Change management 16
6.3 Progressive extension of ICMH scope 17
6.4 Progressive integration into the organization 17
Annex A (informative) Examples of ICMH schemes 18
Annex B (informative) Examples and guidance when applying the ICMH system to information assets in different formats and/or media 23
Bibliography 31

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. 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 171, *Document management applications*, Subcommittee SC 1, *Quality, preservation and integrity of information*.

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

Across all business sectors, there are organizations that already identify, classify and distinguish their own information and electronic communications according to internal rules. This classification is then used to direct the organization’s staff and partners to take pre-agreed steps to use, protect and share the information, appropriate to how the organization values that information.

However, there is frequently no agreed equivalence of such classification, marking and handling among private sector organizations, or across the wider public sector, nor between private sector and public sector organizations. This can result in the organizations involved handling shared information differently and sometimes inappropriately.

This document encourages organizations of any size, and in any business sector, to use a managed and more consistent approach to handling information assets on the basis of their classification and marking. This approach can deliver a significant improvement in how information, and in particular sensitive information, is managed, both within the organization and within other organizations with which the information is shared. It can also contribute to the protection of the organization's investments, income, reputation and future. For example, technology companies involved in the business of information creation (e.g. typesetting or email software) that adopt and integrate the specifications in this document into their solutions will be able to create secure, automated document handling solutions, including monitoring systems, that detect and act upon the transmission of information assets that have been classified and marked.

More specifically, this document is intended to support the design of information classification, marking and handling (ICMH) systems to help organizations:

- meet their strategic objectives, governance obligations and enterprise risk management goals;
- meet legal, regulatory and standards compliance obligations;
- identify, secure, protect, share and track sensitive information appropriately; and
- improve user understanding of the value and significance of information assets and familiarity with their appropriate handling requirements.

Document management — Information classification, marking and handling —

Part 1: Requirements

1 Scope

This document specifies requirements for information classification, marking and handling (ICMH). This document also defines how such information can be accessed by users, both inside and outside the organization, who own the information.

This document is applicable to, but not limited to, the following:

a) organizations of any size that create, store, share or otherwise process information;

b) individuals who create, store, share or otherwise process information;

c) individuals with responsibilities for document management, information governance and management, information security, data protection, privacy and/or compliance; and

d) organizations that create, provide or support tools that enable a) to c).

This document addresses information that can be understood by humans and is capable of being shared. Throughout this document such information is referred to as an “information asset” regardless of its media or format.

NOTE Information assets can include structured information, unstructured information, text, pictures and audio/video recordings, i.e. anything that contains information, including information that is derived from databases and turned into a tangible asset.

2 Normative references

There are no normative references in this document.

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

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

3.1
classification

systematic identification and/or arrangement of *information assets* (3.7) into categories according to logically structured conventions, methods and procedural rules

Note 1 to entry: These categories consider issues such as the sensitivity of an information asset to loss or damage, i.e. confidentiality, integrity and availability and other impacts on the organization(s).

[SOURCE: ISO 15489-1:2016, 3.5, modified — “information assets” has replaced “business activities and/or records” and Note 1 to entry has been added.]

3.2
document
information (3.6) and the medium on which it is contained

[SOURCE: ISO 9000:2015, 3.8.5, modified — the example and notes to entry have been deleted.]

3.3
handling
required activities relating to *information assets* (3.7) that have been marked with a specific *classification* (3.1)

3.4
information classification, marking and handling scheme
ICMH scheme
respective, specific requirements and arrangements established for the individual activities of *classification* (3.1), *marking* (3.10) or *handling* (3.3)

3.5
information classification, marking and handling system
ICMH system
set of interrelated or interacting elements to establish information *classification* (3.1), *marking* (3.10) and *handling* (3.3) policies and objectives with processes to achieve those objectives

3.6
information
meaningful data

Note 1 to entry: Data can be regarded as lacking the context necessary to interpret its meaning. Information is accurate and timely, specific and organized for a purpose, presented within a context that gives it meaning and relevance, and can lead to an increase in understanding and decrease in uncertainty. Information is valuable because it can affect behaviour, a decision or an outcome.

[SOURCE: ISO 9000:2015, 3.8.2, modified — note 1 to entry has been added.]

3.7
information asset
set of *information* (3.6) that is capable of being shared and can be held in any form, e.g. physical or digital

3.8
information asset life cycle
sequence of events that mark the development and use of an *information asset* (3.7)

[SOURCE: ISO 13972:2022, 3.1.40, modified — "information asset" has been added to the term; “asset” has replaced “resource” in the definition; the note 1 to entry and example have been deleted.]

3.9
information provider
individual or entity that has shared *information* (3.6) with the organization

Note 1 to entry: This includes *workers* (3.17) within an organization when, for example, referring to them as natural persons. Otherwise it relates to third parties.

3.10
marking
process by which a *classification* (3.1) is documented and indicated for an *information asset* (3.7) (usually on the information asset)

3.11
metadata
data about data

Note 1 to entry: Metadata (see ISO 23081-1 for further information) is contained in many *information assets* (3.7) and describes the information asset. *Information classification* (3.1), *marking* (3.10) and *handling* (3.3) technologies and tools commonly use metadata to convey classifications. Without the use of such technologies, metadata are not always immediately visible and possibly will not be automatically transferred when the *information* (3.6) changes format.

3.12
physical storage media
physical device on which *information* (3.6) can be recorded

3.13
record
information (3.6) created or received and maintained as evidence and as an asset by an organization, in pursuit of legal obligations or in the course of conducting business

Note 1 to entry: Records are normally used in plural.

[SOURCE: ISO 30300:2020, 3.2.10, modified — note 2 to entry has been deleted.]

3.14
redaction
permanent removal of *information* (3.6) within a *document* (3.2)

[SOURCE: ISO/IEC 27038:2014, 2.4]

3.15
replication
digital duplication where there is no change to the *information* (3.6)

[SOURCE: ISO/TS 21547:2010, 3.1.26]

3.16
storage media
device on which digital *information* (3.6) can be stored

3.17
worker
individual working under the control of an organization, including employees, temporary staff, contractors and consultants

4 Principles

The information classification, marking and handling (ICMH) system shall include a definition of a process that can handle information in a way that is appropriate to its classification and to its marking.

The ICMH system shall:

a) be as simple as the circumstances allow;

NOTE 1 An overly complex process can be difficult for a small company to apply and a simplistic process does not always suit the complexity required in a large organization.

b) reflect the sensible limits of what can be expected of its workers so that they can obtain an appropriate balance of what is necessary, recommended and possible to achieve;

c) produce consistent results upon repeated use, regardless of the user;

d) be traceable and capable of verification;

e) be usable by both human and automated systems;

f) be usable for purely manual processes (e.g. paper-based), as well as fully- or partially-automated processes;

g) address all relevant security attributes;

h) take account of, and where appropriate, replace existing ICMH systems;

i) support compliance with internal and external requirements;

j) be resilient to changes in circumstances, technology and systems;

NOTE 2 The ICMH system tends to augment an original scheme, e.g. with additional descriptors, as the role or coverage of an ICMH system evolves. This does not necessarily mean changing the entire ICMH system.

k) take account of changes in the nature and sensitivity of information over time;

l) be applied throughout the lifetime and life cycle of the information asset.

The ICMH system shall be consistent with the organization's overall information management policies and procedures.

Consideration shall be given to all opportunities to facilitate effective handing which are open to the organization, to facilitate effective handling, including simplifying the arrangements as much as possible and supporting them with technology, as appropriate.

5 ICMH system design

5.1 Classification scheme design

5.1.1 Classification criteria

The ICMH system shall include a specification of a classification scheme, detailing how information shall be classified, and by whom, such that people with authorized access to information can mark and handle the information in a consistent manner.

Information shall be classified in accordance with:

a) the assessed direct and indirect value of the information for the organization(s) involved;

b) the risk of inappropriate disclosure, corruption, or loss of access to the information asset, and the organization’s appetite to accept such risk(s);

c) the related costs for the organization of identified risk events which can occur and result in negative impacts such as harm to members of the public, reputation damage, costs of rectification and of mitigation;

d) the expectations of stakeholders who are not necessarily directly engaged in the information asset but whom nonetheless have the authority to impose requirements;

e) the need to control the extent to which the information asset can be accessed throughout its life cycle;

f) the coherence of the information with, and mapping between, classifications and risk levels of information used in the organization’s risk management process;

g) the amount of effort required to protect the information asset;

h) the specific expectations of other organizations with which information assets are shared;

i) the general expectations of other parties, such as members of the public and journalists, etc., even when the information is not being shared;

j) social responsibility obligations and/or aspirations of the organization.

The ICMH system shall specify what action workers shall undertake if they:

- cannot make an assessment of classification;
- cannot comply with the requirements of the classification, e.g. for legal or practical reasons;
- consider the classification assigned to and marked on an information asset to be incorrect.

Consideration shall be given to its decision regarding the impact of classification changes on the authenticity and/or integrity of the information.

The ICMH system shall define:

- the procedures to mitigate the impact of classification changes on the authenticity and/or integrity of the information;
- the range and extent of changes to classification that workers may perform on each class of information asset throughout its life cycle.

The justification for the classification scheme shall be documented and traceable.

NOTE Annex A provides example classification, marking and handling schemes. Annex B provides examples and detailed guidance when applying the ICMH system to information assets in different formats and/or media.

5.1.2 Hierarchy

Information shall be classified according to a hierarchy. The number of classes in this hierarchy shall be specified.

NOTE 1 Typically, a hierarchy of access restrictions ranges from “restricted access” to “unrestricted access”. For a brief example of a hierarchy, see Table 1. For a more detailed example, see Table A.1.

Consideration should be given to the usability of the hierarchy. In general, fewer classes will be simpler to use and more likely to be used correctly.

The names of the classes in this hierarchy shall be specified.

NOTE 2 One example of a hierarchy can include highly sensitive, sensitive, not sensitive and intended for publication.

The hierarchical classes should have meaningful names. For example, defining a hierarchy of “not sensitive” to “highly sensitive” is likely to be more helpful than defining a hierarchy of numbers “1” to “5”.

NOTE 3 If all information is classified at the highest level, the efficiency of an organization can be reduced. If all information is classified as having unrestricted access, it is likely that this would cause harm to the organization.

Table 1 — Example of a confidentiality hierarchy

Class	Description
Highly sensitive	This information is the most sensitive held by an organization and great care should be taken to avoid it being accessed (accessed rather than shared because sharing implies a conscious act) inappropriately as this can cause great harm to the organization.
Sensitive	This information is not as sensitive as highly sensitive information but can nonetheless do harm if accessed inappropriately.
Internal	This information is private to an organization but unauthorized access to the information within it is unlikely to do significant harm.
Public	This information is intended for public dissemination.
Non-sensitive	All other information or information assets that are not classified as the information in them is trivial and access to it poses no danger to the organization.

5.1.3 Classification scheme equivalence

If, for the purpose of work, the organization shares or exchanges information with a third party, the ICMH system shall:

a) be explained to the third party so that the third party understands the significance of the system and associated schemes and the organization's requirements for classification, whether or not the third party has a classification scheme;

b) be agreed upon by relevant parties. The equivalence between the schemes of the organization and the third party shall be documented, whenever possible;

c) include documentation on how exchanged or shared information is classified and consequently marked and handled by the third party.

When creating or updating a classification scheme, the equivalence of its information classification, marking and handling (ICMH) schemes with the schemes of third parties with whom they exchange or share information shall be preserved.

Consideration should be given to how technology can be used to ensure reliable and consistent mapping between these schemes and enforcement of control rules, and if the rules are conducive to technology use.

5.1.4 Information asset life cycle

The classification scheme shall be continuously applied throughout the information asset's life cycle and shall be managed from creation or capture to eventual disposal, which can be many years later.

NOTE 1 It is not uncommon for there to be changes to the classification of specific information, and consequently its marking and handling, throughout the information asset life cycle organization (e.g. from a high degree of control to lower, more relaxed access control).

Where an expected classification change is pre-planned, the triggers, procedures and organizational rules for such future change shall be preserved. This shall ensure that the information is linked to the appropriate triggers, procedures and rules.

NOTE 2 Changes to classification can be pre-planned or unforeseen. For pre-planned changes to classification, there is typically a trigger that initiates the future re-classification; such a trigger is typically a date, a period or a specific event.