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

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.

The ICMH system shall define the information to be created and retained for planned and unplanned changes in classification of information assets, such that evidence of such changes is available when required.

Where the classification of an information asset is created or changed, the classification history of the information asset should be retained in an audit trail throughout its life cycle. This can include:

— a new classification:
  — date and time of classification;
  — information asset classification;
  — authority for classification;
  — classification time, date and any event-related validity (optional);
  — anticipated future classification (optional);
— a changed classification:
  — date and time of classification change;
  — authority for classification change;
  — preceding information classification;
  — classification validity (expiration) time;
— any anticipated classification changes:
  — trigger for classification change (e.g. time, date, event);
  — likely information classification (category, etc.);
  — authority required for such a classification change;
  — classification (time frame) validity (optional).

The change log information shall be available in a way that preceding and succeeding classifications can be determined together with the current classification and justification for the classification level change.

5.1.5 Default classifications

Consideration shall be given to whether to create and use a default classification. Where a default classification is created, the decision for taking this action shall be documented.

NOTE 1 When creating or using a classification scheme, organizations can find it useful to set a default classification that is appropriate for their general and most used approach to the sensitivity of information, and which reflects the nature of their activities. Legal practices expect to handle more sensitive information assets than retailers. This normally reduces the effort to classify information as only the non-default classification(s) information warrants individual marking. Such a default becomes the classification that is applied to information that is not otherwise, or potentially later classified otherwise, under the classification scheme.

NOTE 2 There can be multiple defaults in an organization, e.g. in specific operational units. For example, the default for the marketing department can be different from that in human resources (HR), where the majority of information is personal and more sensitive than the majority of the marketing information.

NOTE 3 Information with a default classification still warrants appropriate marking and handling.

In the event of an organization creating or using a default classification, the default shall be explicitly included in the documented classification scheme.

When adopting the use of a default classification, consideration should be given to the balance between user convenience and the awareness and accountability that result from users being required to make a positive choice.

5.1.6 Information assets that are not marked

Where an organization decides that it shall allow information assets to be unmarked, and therefore without a specific classification, the ICMH system shall specify what the effective classification, and thus the associated handling, of that information asset shall be.

NOTE 1 The effective classification is frequently the default classification.

NOTE 2 A common alternative to the default classification is typically a "public" classification or similar.

5.1.7 Descriptors and dependencies

The ICMH system shall specify whether descriptors shall be included within their classification scheme and, if so, whether those descriptors shall appear in the marking scheme (see 5.2).

NOTE 1 In some cases it can be useful to apply a descriptor to information to enable anyone handling it to understand something about why it has been classified in a particular way. For example, the handling of some information can be subject to applicable national or international laws, the requirements of a regulatory body, or the strategic business requirements of the organization.

The following are examples of possible descriptors:

a) PII: This information asset contains personally identifiable information (PII) that is expected to be protected under applicable national or international law.

b) Legal: This is information that applicable national or international law is expected to be handled in a certain way, e.g. archived or published.

c) Strategic: This information is of strategic importance to the organization but is not protected under applicable national or international law.

For example, a document can have a marking in the title or footer with a suffix "Sensitive – legal" denoting both the sensitivity and the source of the classification.

d) Structural: This information relates to an identifiable unit or element of the organization, e.g. a business unit, functional activity, project or operation.

The ICMH system shall specify whether dependencies shall be included or addressed within their classification scheme, and if so, whether those dependencies shall appear in the marking scheme. The decisions by the organization should be based on considerations of how likely dependencies are to exist and the outcomes.

NOTE 2 Examples of typical dependencies include the following:

a) Geography: information can have different legal status, significance or security requirements in different locations; any information that is available to the public online can have no geographic dependency unless geo-fenced in some way.

b) Time: information can have different status or significance depending on time and date.

c) Events: a particular event such as a disclosure following a statutory request for information that changes the classification.

d) Aggregation: information can have a different legal status or significance if it is, or can be, aggregated with other information or with data.

e) Approval: information and its classification can require a further evaluation or "sign off" by another party.

Consideration should be given to the number of descriptors and dependencies it needs, if any, and should take account of the impact upon its operations that can result from such complexity.

5.2 Marking scheme design

5.2.1 Marking design criteria

The user shall apply the marking as defined for the particular classification of that information, i.e. the classification shall be shown by a mark.

The mark should be visible to viewers at the point they view it or otherwise experience it and the mark should continue to be visible if the information is replicated, shared with a third party, or converted in format.

The mark should be visible, independent of the viewing/access method.

The language of the mark should be appropriate to the context and operational environment of the ICMH system.

NOTE 1 For example, headers and footers in electronic documents can be suppressed as a default in many document reader or editor programmes. A marking scheme using only headers and footers is not always visible. A mark that depends on a particular programme significantly increases the chance that the classification mark will be "lost" in a change of format of the information.

Where a visible mark is not appropriate, the circumstances for such a decision shall be explicitly defined and documented.

Except when the information asset is for public consumption, having no visible mark should be discouraged.

NOTE 2 "Visible" is used here as being able to be immediately understood according to the format of the information. For example, "heard" for an audio file, "read" for a Braille embosser or "displayed on a screen" for a document.

Marking shall be reviewed every time classification is reviewed. If the organization decides not to revisit all previously marked assets when implementing a change in the scheme, it shall document this decision and communicate the requirements for handling assets classified under the old scheme while the new scheme is implemented.

Metadata shall not be used as a substitute for a mark, but where it is designed for the purpose of classification, it shall be consistent with the visible mark.

5.2.2 Placement and style of marking

The ICMH system shall define the style, placement and structure to be used for marking information assets.

The style, placement and structure of the mark shall be capable of being consistently applied and suitable for the medium or format.

NOTE 1 This document does not mandate how or where marking is placed on visible, audible or other information.

The mark shall be apparent on opening an information asset. Where an identifiable marking is not possible, the circumstances for such a decision shall be defined.

NOTE 2 Not all information is accessed in a strictly linear fashion (e.g. websites). Where such formats and access methods are used, it is quite common that the marked classification of an accessed information asset is not obviously apparent.

The marking scheme, while self-consistent, can vary for different classification levels. Information at the least sensitive level of classification should require the least energy or effort in marking. At the highest level, marking should be subject to additional effort. For example, highly sensitive information can benefit from continuous marking, that is, marking that is always visible at any point where the information is viewed, heard or experienced. This can be through watermarking on documents, an

overlay on video or a continuous tone on audible material. This also ensures that partial views of the information, e.g. a single page in a printed document, still carry the mark. Low sensitivity information should not involve such complex marking so that creators or editors avoid marking it.

The marking of information shall, wherever possible, be automated, and such automation shall prevent the unauthorized deletion, or alteration, of marks on the information.

NOTE 3 Enforcing features can include the mandatory use of permanent ink, marking paper documents and using digital templates that cannot be changed by users.

5.3 Handling scheme design

5.3.1 Handling design criteria

The ICMH system shall define the specific control measures (such as watermarks) required for each individual classification which shall be communicated through its mark.

The classification scheme shall enable an information asset, with a particular classification, to be handled differently when pre-defined conditions exist.

EXAMPLE 1 Such a discrete classification then forms the mechanism for altering the rules surrounding when or who is allowed to access an information asset or special handling arrangements for a given business partner.

EXAMPLE 2 Where the organization concludes that encryption of information assets is required for some classifications and marks but not others; this is made clear to those handling such information.

The organization's handling scheme shall explicitly define which individuals, groups of individuals or business roles can handle the information as well as how they shall handle it.

NOTE The definition of which individuals are entitled to handle information can be by role, by grade or individually as circumstances or organization preferences require.

When necessary, the suitability of particular individuals should be verified in accordance with the organization's HR policies and procedures. ISO/IEC 27001:2022, Annex A, provides relevant information.

The ICMH system shall specify:

a) what automated processing is allowed for marked information assets;

b) what classifications of information can be created on what collaborative platforms;

c) when working versions of information assets shall be retained, in what form and for how long;

d) a process for documenting and responding to known instances of mishandling information with regards to its classification, consistent with the organization's document management system.

5.3.2 Information handling during creation and capture

The ICMH system shall specify what information shall be created, captured and/or modified by which individuals and what approvals are required, and from whom.

The ICMH system shall specify that information is classified at the point of creation or capture (e.g. by filming) in accordance with the classification scheme (see 5.1).

The ICMH system shall define the production specifications for all classifications.

EXAMPLE 1 Where the asset is a text document, these specifications typically include page formats and pagination, page numbering, the style of such numbering, copy numbering, the positioning of such numbering and handling of blank pages.

Where an information asset is reformatted, held in a different software application or on a different type of physical storage media, different appropriate specifications should be applied.

If required for any given classification(s), the ICMH system shall maintain a log of the handling of the classification, as well as the marking and handling of information throughout the information asset's life. This typically applies to classifications that relate to particularly sensitive information assets.

NOTE 1 If copy numbering is required, it is likely to be for the purpose of recording the recipients. In such circumstances, it is appropriate to store this is in the information, in addition to the log.

NOTE 2 The log is therefore initiated at first creation, i.e. the log document is actually the first item created.

When the creation of an information asset is considered to have been completed, the creator shall reassess the asset's classification, and consequently if or how the associated marking and handling shall change.

5.3.3 Information re-use in other information assets

The ICMH system shall create a process for managing the appropriate reuse of an information asset, parts of information assets or in other information assets. The process shall make clear:

a) the permissions and approvals which are required;

b) how the information is then classified, marked and handled.

5.3.4 Editing and changes to an information asset

When an information asset is edited or changed substantively, the information asset's classification shall be reassessed, and consequently any necessary changes to the marking and handling of the information asset shall be made.

The ICMH system shall define what constitutes a substantive change.

NOTE Changes include the general editing, addition, alteration, substitution or deletion of some or all of the information in the asset.

5.3.5 Information aggregation

The ICMH system shall specify how information that is aggregated, or inferred, from other information is then classified, marked and handled.

NOTE 1 Combining information from several sources can result in information with a different classification. The same is true when information is disaggregated. A simple example of where combining information from different sources alters the classification, and thus the marking and associated handling, is when a list of products that have been sold is combined with a list of customer names.

The ICMH system should take into account that, in an age of "big data", the combination of information from various sources can create, sometimes accidentally, "personally identifiable information" which should then be subject to additional specific protections. See B.10.4 for a further example of this.

NOTE 2 Combining information with different levels of classification is likely to result in the aggregated information asset carrying at least the most sensitive marking of the source set.

5.3.6 Access to and handling of information

The ICMH system shall define and apply logical and/or physical access permissions and controls for the information, based upon the classification. The ICMH system shall specify how these are granted and managed.

NOTE 1 Permissions can require the use of passwords and user authentication, e.g. rules about remote access (both whether access is permitted and how access can be achieved), the use of data rooms, and location constraints such as where the information can and cannot reside, physically or virtually.

The ICMH system shall define the handling rules, related to each classification, for the removal of information from physical and digital storage media.

The ICMH system shall identify when, under what circumstances, and how, an information asset can be taken out of physical locations under the organization's control within a given geography, taken between geographies and when it can be moved between different legal jurisdictions.

In the event that there are changes to the classification scheme or the classification (and mark) associated with a specific information asset, the access, sharing and editing rights of a worker to that asset shall be reviewed and the changes documented.

Where required, and especially its classification and handling schemes, the ICMH system shall specify that those access rights enable and enforce any limitations set upon the "need to know" principle.

NOTE 2 It can be useful to divide information as much as possible to limit the accessible range of information, subject to not over-complicating the classifications, marks and handling criteria.

Consideration should be given to whether the logging of all access history is an appropriate element of its handling scheme for any of its classifications.

5.3.7 Information storage

The ICMH system shall define the rules for the storage of marked information assets.

NOTE 1 Storage rules can include the types, ownership, security, connectivity and locations of operating systems of devices that can be used to store information of a particular classification. For example, an information asset can be stored on an encrypted laptop but not on a USB stick, another information asset can only be stored on servers within a particular location, while another information asset can be stored on public cloud or other sharing platforms.

NOTE 2 For example, while marking a textual document is relatively easy, producing information in audio and/or video that is stored containing an overlay marking or tone, which cannot subsequently be removed or altered, can be complex and more difficult. The organization can consider the cost of marking audio and/or video files and the benefits accrued by such marking in addressing storage and handling issues.

Retention of information in systems intended for secure storage and presentation can be treated, by default, as denoting the sensitive nature of the information. For such circumstances, the ICMH system shall document and communicate that such information shall be deemed to have been marked and shall be treated as being stored securely. Information in such systems shall either be prevented from being deleted, altered, extracted, shared or otherwise processed.

EXAMPLE An audio recording of a conversation containing sensitive information is available on a company intranet. The visible screen can display the required marking information while the audio file itself does not contain audible marking information. If the same information is removed from the source system and transmitted elsewhere, then it is expected that the audio itself has the security information contained within it.

5.3.8 Information replication and rendering

When an information asset is copied, replicated or rendered in a different format or media, the classification rules shall remain unaltered. Marking and handling, however, do not necessarily remain unaltered.

Where required by the handling requirements of the ICMH scheme for specific information assets, the individual copying, replicating or rendering processes shall report the process undertaken. The evidence showing the implementation of these processes shall be recorded in the audit trail.

The marking and handling rules for the replicated or rendered information asset shall follow the ICMH system for the appropriate format or media, which can be different from the previous set of rules.

EXAMPLE 1 When an electronic information asset is converted (e.g. from a word-processor document format to a PDF) or printed (i.e. it becomes available in a form which is no longer electronic).

If replication or rendering causes the information to be created in a new form, the handling rules for that information asset shall be defined within the handling scheme.

Where such replication is in physical form, such as printing, faxing or photocopying, the ICMH system shall define the handling rules that shall be applied, including whether or not the replication can take place in an insecure location.

EXAMPLE 2 When replication takes place at a remote location, such as a fax machine or networked printer, the person responsible for the replication informs an appropriate person in the remote location to attend the device and physically secure the output.

For any given classification(s), the ICMH system shall specify when an audit trail of any copying, replication or rendering is required. Where required, the audit trail requirements shall be specified and included in the documented information.

NOTE The documented information about replication can include what is being replicated, who is replicating it, why it is being replicated, when they are replicating it, where they are replicating it and the replication medium used.

When an information asset is replicated, the classification and marking shall be maintained in the replicated version.

Where the information asset is replicated (for example when an online information asset is printed) in a different physical form, the mark style appropriate for the new physical form shall be used.

The ICMH system shall define the instances, if any, in which an information asset, which has been classified and marked, can be reproduced without a classification mark.

EXAMPLE 3 A marketing document is classified and marked "public" during its drafting but the marking is then dropped upon actual publication, although the handling behaviours remain in place.

5.3.9 Information redaction

When an information asset is redacted, the information asset's classification shall be reassessed. Following this review, any necessary changes shall be made to associated marking and handling.

NOTE 1 Some information assets with appropriate classification can contain information that is not supposed to be disclosed to some recipients.

Modified versions, with differing classification, marking and handling arrangements, should be released to these recipients after an appropriate processing of the original version. This processing can include the removal of sections, paragraphs or sentences with, where appropriate, the mention that they have been removed. This process is called the "redaction of the information asset".

The ICMH system shall treat a redacted version of an original information asset as a new information asset.

NOTE 2 Redaction can also involve the removal of information asset metadata or the removal of some information (e.g. an image).

Where an information asset shall be digitally redacted, the processes and procedures used shall ensure that the redacted and removed information is not recoverable from the redacted information asset or from the redaction system.

NOTE 3 With many commercially available digital tools, the information can be simply hidden within non-displayable portions of the information asset and can be recoverable, which would defeat the objective of the redaction process and the consequent re-classification of the information asset.

NOTE 4 ISO/IEC 27038 gives more details concerning methods for digital redaction.

5.3.10 Information distribution, sharing and exchange

The ICMH system shall define whether an information asset with a particular classification may be distributed or shared and if so with whom, how and under what circumstances. Such sharing rules shall address the handling rights and responsibilities of recipients.

The organization distributing an information asset, or who are party to an exchange or sharing of information, may opt or be required to use given classification(s) to create and maintain an inventory of information assets sent and received.

The handling rights of all users, including recipients, should include whether they are entitled to further share the information asset and how. For example, it should be specified whether it is permitted to use the "forward" function that exists in most email systems.

NOTE 1 Mechanisms, such as secure collaboration platforms, can manage this, often supporting the standardized Traffic Light Protocol (TLP) as given in ISO/IEC 27010.

The ICMH system shall identify the type of medium(s), such as USB sticks, cloud-based information exchange services, instant chat and messaging platforms, that are allowed for distribution or sharing.

NOTE 2 Where a classification requires that the information asset cannot be shared, suitable technical measures for reducing the possibility of copying can be used. Examples of such technical measures include using media that cannot be copied (e.g. USB memory with copy guard, digital rights protection solutions, or electronic data that is set to prohibit copying, printing or recording).

Where sharing platforms are not approved, the ICMH system shall prohibit their use and shall either provide equivalent facilities that are approved and capable of being trusted, or specify what alternative mechanisms are approved.

The ICMH system shall define the types of distribution channels, such as mail and email, which are permitted for each classification.

The ICMH system shall specify what the precedence arrangements are for its handling scheme versus the handling schemes of any formal sharing or disclosure scheme in which it participates.

5.3.11 Information archiving and disposal

In a manner consistent with its overall information and document management policies and procedures, the ICMH system shall specify what versions of information assets shall be kept, in what form, where and for how long.

The ICMH system shall have policies and procedures for the tracing, capture and disposal of all other copies or versions of information assets.

The ICMH system shall specify how information assets with different classifications, and the media in which they are stored, are deleted, erased or destroyed.

These procedures should address such matters as who authorizes the archiving and disposal and who can perform such tasks. For example, there are many third parties who offer shredding and disposal services that can be considered sufficiently secure for given classifications.

The ICMH system shall specify how logs and other evidence are retained and when and how they are disposed of.

Dependent upon classification or an information sharing agreement, the information recipient shall record the disposal method and disposal result, reporting this to the information provider when requested.

NOTE ISO 15489-1 contains information on concepts and ISO 16175-1 contains information on functional requirements with respect to archiving and secure disposal of information assets. ISO/TR 21946 provides useful information on the process of appraisal.

5.3.12 Information security

The ICMH system shall define within its handling scheme, the information security rules to be associated with each classification.

NOTE This can include encryption at rest or in transit, digital rights management, data loss prevention, or secure storage, packaging and carriage rules.

EXAMPLE 1 The hard disk of a laptop contains information that only the HR Director has permission to access. If the laptop is subsequently used by someone else, it is important to define and implement rules surrounding the deletion of that information from the laptop, including rules about the method of deletion.

The ICMH system shall define within its handling scheme, the encryption rules, if any, to be associated with each classification, including classifications for information when in transit.

EXAMPLE 2 There can be a requirement to encrypt personal information when it is taken outside office premises or when it is stored on particular devices such as USB sticks.

5.4 ICMH system evaluation

5.4.1 Evaluation programme

The ICMH system shall define an ongoing evaluation programme that shall be implemented immediately following the initial implementation of the ICMH system.

The evaluation programme shall ensure that:

a) the classification marking and sharing schemes are being operated by all creators, capturers and users of information within the scope of applicability chosen by the organization;

b) such use complies with the relevant policies and procedures of that organization, i.e. that ICMH is being carried out correctly;

c) appropriate information is collected to identify deficiencies and facilitate the ICMH system revision (see Clause 6).

5.4.2 Monitoring and testing

The ICMH system shall define the criteria against which the suitability and effectiveness of the ICMH system shall be measured.

The ICMH system shall define the criteria for ensuring and evaluating the compatibility of and interaction with different ICMH systems within the organization, and between it and other organizations.

The ICMH system shall also define the activities to be undertaken to monitor and/or test the operation of the ICMH system.

NOTE Many organizations have found it useful to maintain an assessment of the maturity of its ICMH systems. Such assessments normally cover such considerations as:

a) the degree of coverage of the information assets within the scope of the ICMH system;

b) the understanding and commitment of the personnel within scope;

c) the accuracy and completeness of the ICMH undertaken;

d) the extent to which technology is enabling or obstructing the attainment of the goals of the ICMH system;

e) the (mutual) effectiveness of ICMH arrangements when information assets are being exchanged with others.

5.4.3 Auditing and assurance

The ICMH system shall specify the independent performance evaluation which shall be undertaken, if any. This shall be considered alongside self-evaluation of performance that is carried out by individuals with ICMH system management roles and responsibilities.

NOTE The scope of such auditing is likely to include all aspects of the ICMH system, including its application to the organization's information assets plus the evidence included in various logs.

5.4.4 Measurement

The ICMH system shall specify what metrics shall be collected about the operation of the ICMH system, at what frequency, by whom and to whom they will be reported.

NOTE It is likely that such measurements will form new operational reporting requirements merged into existing reporting arrangements, wherever possible.

5.4.5 Incident management and investigation

In order to support the proper management of information and to facilitate continuous improvement, the ICMH system shall be specifically reviewed and reported upon, and the ICMH aspects of all security incidents reported to the ICMH system.

5.4.6 Reporting and lesson learning

The ICMH system shall specify that there is effective, periodic reporting, ultimately to top management, on the suitability and effectiveness of the ICMH system.

The ICMH system shall specify that this reporting draws out lessons to be learnt and requirements for improvement by, at a minimum, documenting causes and deficiencies.

Such reporting should encompass 5.4.2 to 5.4.5 and be designed to facilitate continual improvement (see Clause 6).

6 ICMH system revision

6.1 Scheme revision

The ICMH system shall specify that any deficiencies in the respective ICMH schemes are corrected and the changes implemented as soon as practical, in full accordance with the ICMH system. The ICMH system however shall also maintain the capability to make changes to the ICMH schemes if circumstances require it.

EXAMPLE Changes due to legislative or regulatory requirements.

In the event that there are changes to the overall information classifications, the classification associated with a specific information asset, or of the access rights of an individual to that asset, such changes shall be documented.

6.2 Change management

The ICMH system should continuously monitor and maintain its operational context document to capture any material changes.

6.3 Progressive extension of ICMH scope

Where the ICMH system is initially applied to a part of the organization and/or some but not all information exchanges, consideration shall be given to developing, documenting and executing a "roadmap", or similar, for the progressive extension, if any, of the ICMH system.

NOTE It can appear that some parts of an organization do not require any form of ICMH system. The roadmap can be used to recognize and document this. However, an alternative view is to assume that all areas of the organization have at least a minimum level of requirement for ICMH (using defaults, no marks, etc.). This means that they fall in scope of the minimum level of requirement and can have the ICMH system deployed to them sooner than more complex areas of the organization.

6.4 Progressive integration into the organization

The ICMH system shall maintain a focus on the progressive integration of the ICMH system into the organization's operations.

EXAMPLE 1 New IT systems are planned for acquisitions that, if selected with the ICMH system in mind, are capable of more effective enablement of ICMH.

EXAMPLE 2 New operational processes are designed to more effectively support ICMH.

Annex A
(informative)

Examples of ICMH schemes

The example schemes given in Tables A.1 and A.2 are provided solely to illustrate the application of the concepts outlined in this document and are not recommended for immediate adoption, although they can be a useful contribution or starting point.

It should be noted that while these examples use five levels of classification, these are by no means mandatory and can be excessive.

This example indicates an organization that prioritizes confidentiality over availability or integrity. If those other aspects had been of higher priority, the ICMH schemes would look different.

Table A.1 is an example of a "desktop reminder" that can be provided in the form of mouse mats and posters, for example.

Table A.2 is an example of a detailed information handling scheme. It expands upon Table A.1 while also demonstrating all aspects of this document and its interrelationship with the Traffic Light Protocol (TLP) as defined in ISO/IEC 27010:2015, Annex C.

The approach taken for Table A.2 is to highlight where there was a requirement only. This means the absence of specific requirements are not stated. For example, information classified, marked and handled as "public" can be physically disposed of in any way that is convenient, i.e. it requires neither "simple, but controlled, shredding" nor "cross- cut/dematerialized shredding", both of which are considered unjustified by the high cost of the equipment and the number of such devices that would be required.

Table A.1 — Example classification and marking scheme

Classification	Risk relevant level	Related mark	Impact description	Examples	Essence of sharing and handling rules
Highly sensitive	Very high	Highly sensitive	Severe impact on the financial sector and/or economy or political policy. Costs and severe embarrassment, making a public response obligatory. Viability of organization and partners threatened.	Strategic plans Security and other configurations Credit limits Fraud data Commercial data Corporate policy papers	Documenting of all changes made to information content, classification, marks and handling. Not for sharing, unless edited "down" before release. Typically not mailed but securely downloaded, not onto mobile media. Stored in encrypted form. Secure printing, to be "pulled" by user. Presumed to be material requiring archiving/extended retention.
Sensitive	High	Sensitive	Impact on financial sector and embarrassment for partners. Costs per organization. Regulator formal investigation and enforcement action likely.	Processing rules Process documentation Solution design detail Intellectual property Reports and analyses	Extremely limited sharing, with a minimum number of named individuals by secure routes for constrained use. Circulation lists. All pages marked "Default level" for all HR information. Descriptors used to denote main purpose e.g. "alpha project". Secure disposal and media sanitization.
Limited	Medium	Limited	Harm and nuisance measurable and above an agreed limit. May or may not become public. Duration of any breach likely to be limited in duration and impact is only on the organization itself.	Risk register and plans Organization charts Personal identifiable information Meeting minutes Draft public materials	Sharing among a group which meets defined criteria, with confirmed "need to know". All partner information to be classified at this level or higher. Documents marked on front page. Contractual or conduct agreement for all in the group. Secure physical storage. Controlled document disposal.
Internal	Low	No mark	Minor harm and nuisance if disclosed, without any meaningful level of embarrassment and only minor recovery costs.	Handbooks, newsletters Ops announcements Policies and standards Directories Meeting agendas	For general use within the originating organization. All unmarked information that is not public to be classified and handled at this level. Use only in controlled locations. Not for local storage. Strong passwords on local devices.

Table A.1 *(continued)*

Classification	Risk relevant level	Related mark	Impact description	Examples	Essence of sharing and handling rules
Public	None	No mark	No harm possible to any party.	Marketing material Adverts Public statements Websites Publications	No limit upon sharing, but may or may not have been designed for the purpose. Still to be stored on corporate systems and backed up. No transmission constraints or other specific requirements.

Table A.2 — Example handling scheme

Classification level		Highly sensitive	Sensitive	Limited	Internal	Public
Marking, creation and use	Public release mark during drafting					Y
	Mark when circulated				Y	
	Mark on front page			Y		
	Mark on all pages	Y	Y			
	Pages numbered			Y	Y	Y
	Page "N" of "N"	Y	Y			
	Copies numbered and assigned	Y	Y			
	Formal document	Y				
	Information author and user clearances	High	Medium	Medium	Low	None
	Simple redaction permitted		Y	Y	Y	
	Specialist redaction process only	Y				
	Approval of original author for re-use	Y	Y			
	Machines used to process and display information also marked	Y	Y			
Logical access	Strong passwords	Y	Y	Y	Y	
	Remote access two-factor authentication		Y	Y	Y	
	Two-factor authentication for all access	Y				
	Personal device use			Y	Y	Y
	Corporate devices only	Y	Y			
Storage/data security	Encryption at rest	Y				
	Locations with site and building access control			Y	Y	
	Locations with room access control	Y	Y			
	Not taken outside pre-agreed locations	Y	Y			
	Secured filing and storage	Y	Y			
	No mobile storage device/media	Y				

Key

Y Yes

N Not applicable

[a] SharePoint is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

[b] DropBox is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

Table A.2 *(continued)*

Classification level		Highly sensitive	Sensitive	Limited	Internal	Public
Distribution and sharing	Code of conduct between parties	Y	Y	Y		
	Need to know			Y	Y	
	Formal sharing definition (who and why)	Y	Y			
	Sharing protocol level	N	Red	Green	Green	White
	Internal email only	Y	Y			
	External email			Y	Y	Y
	Emailed, with no forwarding capability			Y		
	Instant messaging and social media					Y
	Download only from SharePoint[a], etc.	Y	Y			
	Chain of custody	Y				
	Pre-approved sharing platforms		Y			
	Public sharing platforms (e.g. DropBox[b])			Y	Y	Y
	Usually not shared	Y				
	Encryption in transit	Y				
	Directly owned or dedicated IT	Y	Y	Y	Y	
	Printing “pulled” or attended	Y	Y			
	Faxed to unattended machines					Y
	To attended machines, pages counted		Y	Y	Y	
	Not faxed	Y				
	Postal service			Y	Y	Y
	Secure courier	Y	Y			
Disposal	Pre-approval of information owner	Y	Y			
	Check for archiving and retention	Y				
	Simple, but controlled, shredding			Y	Y	
	Cross-cut/dematerialized shredding	Y	Y			
	Periodic review and cleanse of storage		Y	Y	Y	Y
	Regular purge of IT storage	Y				
	Media erased				Y	Y
	Media sanitized/degaussed		Y	Y		
	Media physically destroyed	Y				

Key

Y Yes

N Not applicable

[a] SharePoint is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

[b] DropBox is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

Annex B
(informative)

Examples and guidance when applying the ICMH system to information assets in different formats and/or media

B.1 General

This annex provides examples and guidance on particular challenges that can arise when information is created and then stored or used in different formats and/or media. The following formats and/or media are covered:

— paper-based information;

— electronic documents and digital files;

— film and tape;

— voice;

— images;

— mobile working;

— assistive technology;

— collaborative platforms;

— database tools;

— websites, internet and intranets;

— social media.

B.2 Paper-based information

B.2.1 Creating paper-based information assets

Paper-based information assets should be treated with the same consideration as digital assets. The advent of electronic information handling does not lower the sensitivity and/or value of paper-based information.

NOTE The creation of a new information asset on paper typically involves the use of a blank sheet but it can use a sheet (or bound page) that already contains information.

When creating and handling information assets on paper, the following should be taken into account:

a) Whether all sheets of paper with information documented upon them should be classified and marked (unless default classifications and/or not marked assets are allowed in the ICMH system, see 5.1.5 and 5.1.6).

b) Information on originally blank paper can be drafted and redrafted several times, with commensurate changes in the information's sensitivity. Care should therefore be taken to ensure that any drafts, classified as needing protection, are securely handled commensurate with the classification and marking of that draft (see 5.3).

c) Adding information to a document that is not classified as requiring any specific protections can result in a document that needs protection and therefore involves appropriate re-classification, marking and handling.

EXAMPLE 1 A meeting agenda carries a low classification marking. However, when notes are added, the agenda becomes a new, or enhanced, information asset that needs additional handling protection, as signalled by a higher marking.

d) Where a pen or pencil is used to create a paper document, it is possible that an imprint (effectively a copy) of the information is left on any sheets underneath or sheets that are later placed on top. These imprints should also be handled commensurately.

The organization can consider providing its workers with resources such as notepads, pre-marked with classifications to bring the required handling behaviours to the attention of workers. However, consideration should be given to the practicalities of the proposal to ensure that the benefits are not outweighed by the operational costs.

EXAMPLE 2 Carrying several notepads can be inconvenient and onerous, especially if information related to a specific project is also required to be documented separately, which can be signified by a descriptor or dependency (see 5.1.7). This can then become further complicated by the handling rules, such as physical transportation and storage of those notepads.

B.2.2 Copying and reproducing assets

Paper documents can be copied in a number of ways. The following should be taken into account:

a) the possibility that photographs of documents can be taken, either by people working on the document who perhaps want an unofficial document, or by people (such as journalists) who are interested in the content of a document being carried by a person of interest;

b) the use of private hand-held scanning devices that can scan documents as images or, in the case of optical character recognition software, as editable text;

c) the use of photocopiers where:

1) documents can be copied incompletely, e.g. without classification marks being copied or with certain pages left out;

2) pages of documents that are being copied can become stuck in the photocopier and discarded carelessly;

3) the use of machines with storage capabilities where the recipient can be unaware that the document is being sent, resulting in the document remaining in the machine;

d) the use of printers where these are in an unsecure location, e.g. workers' homes or public printing services, where adequate data destruction technology is possibly unavailable.

B.2.3 Using, sharing and transporting paper-based information assets

The existence of information assets on paper in visible locations, e.g. on a worker's desk, particularly when not in active use, should be addressed by the organization creating and using it, within their ICMH system.

The handling scheme should address all stages and states of the life cycle of a paper-based information asset (see 5.3.7, 5.3.10 and 5.3.11).