BS 10010:2017

BSI Standards Publication

Information classification, marking and handling —

Specification

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

Published by BSI Standards Limited 2017

ISBN 978 0 580 91832 2

ICS 01.140.20; 03.100.99; 35.240.30

The following BSI references relate to the work on this document:
Committee reference IDT/1
Draft for comment 16/30330940 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

Summary of pages

This document comprises a front cover, and inside front cover, pages i to iv, pages 1 to 37, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 March 2017. It was prepared by Panel IDT/1/-/6, *Protective Marking for Documents and Communications*, under the authority of Technical Committee IDT/1, *Document Management Applications*. A list of organizations represented on this committee can be obtained on request to its secretary.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is “shall”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Requirements in this standard are drafted in accordance with *Rules for the structure and drafting of UK standards*, subclause **J.1.1**, which states, “Requirements should be expressed using wording such as: ‘When tested as described in Annex A, the product shall ...’”. This means that only those products that are capable of passing the specified test will be deemed to conform to this standard.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

Across all business sectors, there are organizations that already identify, categorize and distinguish their own information and electronic communications according to their own internal rules. This is then helpful in directing 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 amongst private sector organizations, or across the wider public sector, nor between private sector and public sector organizations. This leads to information that is shared between organizations being handled differently and sometimes inappropriately (excessively or, more often, inadequately).

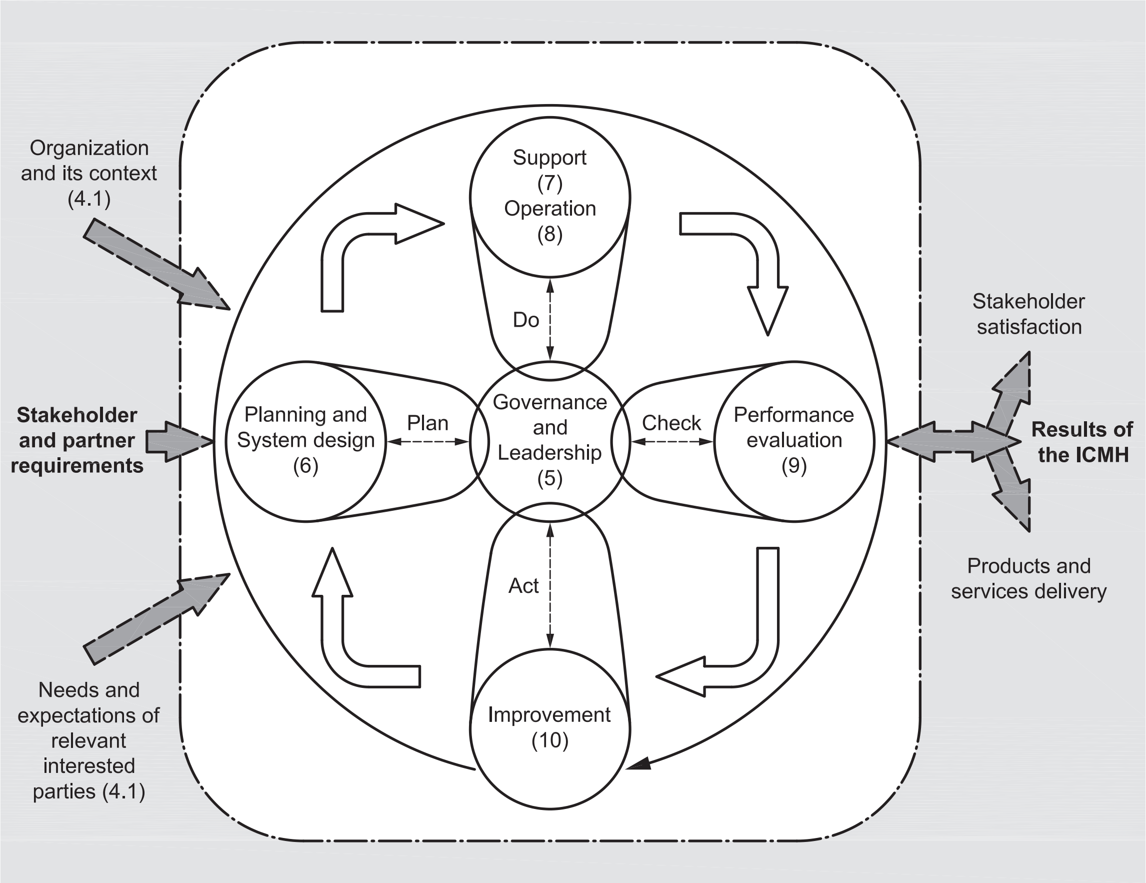
This British Standard intends to encourage organizations, of any size, to use a managed, and more consistent, approach to handling Information Assets on the basis of their classification and marking. This can deliver a significant improvement in how sensitive information is managed, both within the Standard users’ own organization, as well as those 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 content of this British Standard into their solutions, will be able to create 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 British Standard is intended to support organizations to:

- meet their strategic objectives, governance obligations and enterprise risk management goals;
- meet legal, regulatory and standards compliance obligations e.g. Data Protection, BS ISO/IEC 27001;
- secure, protect and share sensitive information appropriately; and
- improve user understanding of the value and significance of Information Assets and familiarity with their appropriate handling.

Information classification, marking and handling (ICMH) requires a systematic approach that essentially conforms to the 'Plan Do Check and Act' (PDCA) cycle as given in BS EN ISO 9001. Figure 1 illustrates how BS 10010, Clause 4 to Clause 10 relates to the PDCA cycle.

Figure 1 — *The ICMH Plan, Do, Check and Act (PDCA) Cycle*


Organization and its context (4.1)
Stakeholder and partner requirements
Needs and expectations of relevant interested parties (4.1)
Support (7) Operation (8)
Do
Planning and System design (6)
Plan
Governance and Leadership (5)
Check
Performance evaluation (9)
Act
Improvement (10)
Stakeholder satisfaction
Results of the ICMH
Products and services delivery

NOTE 1 Based on BS EN ISO 9001:2015, Figure 2.

NOTE 2 Numbers in brackets refer to the clauses in this British Standard.

1 Scope

This British Standard specifies requirements for the creation, implementation, evaluation and improvement of Information Classification, Marking and Handling (ICMH) systems. It specifies requirements for classifying information, including defining how it may be accessed by users, both inside and outside the organization, that own the information.

The intended users of this British Standard include, but are by no means limited to, the following:

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

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

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

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

The scope of this British Standard addresses information that is in a form that can be understood by humans and is capable of being shared. Throughout this British Standard such information is referred to as an 'Information Asset' regardless of its media or format.

NOTE 1 Information Assets can include structured information, unstructured information, text, pictures and audio recordings, i.e. anything that contains information.

NOTE 2 The content of databases do not as easily fit within the marking aspects of this British Standard. However, information in whatever form that is derived from a database and turned into a tangible asset is included within this British Standard, as is information that is not originally derived from a database.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

3.1 classification

systematic identification and/or arrangement of Information Assets into categories according to logically structured conventions, methods, and procedural rules

[SOURCE: derived from BS ISO 15489-1:2016]

NOTE These categories consider such issues as the sensitivity of an Information Asset to loss or damage, i.e. confidentiality, integrity and availability.

3.2 storage media

device on which digital information can be recorded

[SOURCE: PD ISO/TR 17797:2014]

3.3 disposition

range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments

[SOURCE: ISO 15489-1:2016]

3.4 document

recorded information or object which can be treated as a unit

[SOURCE: BS ISO 15489-1:2001]

NOTE As such, a document (which can be written, typed, spoken, viewed) is capable of being created, stored, communicated or shared.

3.5 handling

required activities relating to Information Assets that have been marked with a specific classification

3.6 ICMH System

set of interrelated or interacting elements of an organization to establish information classification, marking and handling policies and objectives with processes to achieve those objectives

[SOURCE: derived from the definition of a management system in BS ISO 30300:2011]

3.7 information

meaningful data

[SOURCE: BS EN ISO 9000:2015]

NOTE 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.

3.8 Information Asset

set of information that is capable of being shared and can be held in any form e.g. physical or digital

3.9 information lifecycle

sequence of events that mark the development and use of an information resource

[SOURCE: BS EN ISO 13119]

NOTE Information resources, in respect of this standard, are Information Assets.

3.10 marking

process by which a classification is recorded and indicated for an Information Asset (usually on the Information Asset)

3.11 physical storage media

physical device on which information can be recorded

NOTE The information might not be in a digital form, e.g. a printed document where the medium is paper

3.12 record

information created, received and maintained as evidence and as an asset by an organization or person, in pursuance of legal obligations or in the transaction of business

[SOURCE: BS ISO 30300:2011]

NOTE 1 An important characteristic of a record is that it has not been altered.

NOTE 2 The term "evidence" is not limited to the legal sense.

NOTE 3 Records can be in different formats and on different media (including paper, disk, removable storage/USB, CD, DVD, digital or analogue tape) and includes documents, email (in the email text, as an attachment to an email or both), video, image and audio.

3.13 redaction

permanent removal of information within a document

[SOURCE: BS ISO/IEC 27038:2014]

3.14 render

action of converting a resource to a human-perceivable form

[SOURCE: BS ISO/IEC 21000-19:2010]

3.15 replication

digital duplication where there is no change to the information

[SOURCE: DD ISO/TS 21547:2010]

3.16 scheme

respective, specific requirements and arrangements established for the individual activities of classification, marking or handling

3.17 top management

person or group of people who directs and controls an organization at the highest level

[SOURCE: BS EN ISO 9000:2015]

NOTE If the scope of the ICMH system covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.18 worker

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

[SOURCE: BS 10008:2014]

4 Context of the organization

4.1 Context and operations

To develop an appropriate ICMH System, the organization shall ensure that it has an up to date definition of its context and of its operational environment that is documented and formally adopted.

NOTE This should as a minimum define the following:

a) the objectives and strategy of the organization, along with its values and vision for itself, and its present reputation, that it will want to defend and/or enhance;

b) its business functions and activities;

c) the manner in which those functions and activities operate and locations used;

d) the constraints of, and within, those processes and practices;

e) the technologies being used, and planned in the short term, to underpin and perform those processes and practices; and

f) the stakeholders with which it interacts and the subset of these, if not all, with whom it exchanges information.

The organization shall ensure that this organizational profile is approved by the organization's top management, such that it can be used to validate that the ICMH System subsequently designed is appropriate (see 5.2).

4.2 Inter-organizational ICMH co-ordination

As part of understanding its context, the organization shall develop a mapping of the organizations with whom it has a requirement to share information, and especially their approach to enterprise risks which might differ from its own.

The organization shall understand the ICMH requirements (and associated systems) of the organizations that it will be sharing information with.

5 Leadership

5.1 Accountability

The top management of the organization shall define and document who will be ultimately accountable for the design, development and operation of the ICMH System.

5.2 Setting direction

The top management shall unequivocally define and document its expectations of the ICMH System, e.g. in terms of reporting to the top management and, on the basis of the context document (see 4.1) and inter-organizational co-ordination needs (see 4.2), give its direction as to what elements of the organization shall be covered by the ICMH System.

5.3 Leadership and management commitment

The top management of the organization shall demonstrate leadership in the operation of the ICMH System.

NOTE 1 This might be, for example, by being part of any first wave of deployment or ensuring that all of the top management's own activities are encompassed within that first wave of deployment.

NOTE 2 Recognizing the normal sensitivity of its activities, the exclusion of top management activity from the ICMH System would, in fact, actively undermine commitment to the ICMH System.

5.4 ICMH policy

The top management shall ensure that an ICMH policy is developed, consistent with the principles given in 6.2, that will be formally adopted, implemented and communicated. In part to demonstrate leadership and management commitment (5.3), but also to facilitate the ICMH System's success, the organization's top management shall communicate a short statement concerning its ICMH policy.

NOTE 1 Such a policy is then available for widespread communication within the organization and for sharing with those it exchanges information with.

NOTE 2 This policy statement would typically be of the form often seen displayed in office kitchens etc. in relation to information security, health and safety, etc.

5.5 Authority

Authority for the management of the ICMH System shall be explicitly allocated by the Top management.

NOTE 1 Typically, this should be to a member of the organization's top management or a department (or function) within the organization that already has sufficient, and associated, subject matter authority, to enforce the use of the ICMH System within the defined scope of applicability and address any queries or discrepancies found from the application of the ICMH Schemes.

NOTE 2 In a small organization this might be the owner or the directors themselves. For larger organizations they might choose to follow their own management structure, where there is clearly devolved authority, or they might already have named responsible persons such as a Chief Legal Officer for legislative requirements, a Compliance Officer for regulatory requirements, a Chief Information Security Officer or a Chief Risk Officer.

The organization shall appoint at least one identifiable person to perform a co-ordination and advisory role.

NOTE 3 The organization should decide whether this role is limited to providing advice or guidance, or have a wider remit in terms of training or authority to classify information.

NOTE 4 Where there is more than one such role holder, the organization should ensure that they meet regularly and exchange information. Such meetings should be planned and perhaps take the form of an ICMH forum or similar.

NOTE 5 Specific roles and role holders might include data protection officers, privacy guardians, security officers, legal representatives or individuals responsible for Information under the Freedom of Information Act [1].

6 Planning and system design

6.1 System applicability

The organization shall explicitly define and document the applicability of the ICMH System, based upon the context document (see **4.1**) and the policy direction (see **5.2**).

NOTE 1 The applicability statement might need to address each of the context document elements in turn to make clear what is and is not in scope.

NOTE 2 It might be the case that there will be a progressive applicability, which should therefore be made explicit.

*NOTE 3 Especially where the system applicability is simple or straightforward to define, it could be communicated as part of the ICMH Policy (**5.4**).*

6.2 Principles

The organization shall define and document a process for creating a system for the handling of information in a way appropriate to its classification, to be communicated through its marking.

The organization shall ensure that its ICMH System:

a) is as simple as the circumstances allow;

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

b) reflects the sensible limits of what can be expected of its workers to achieve an appropriate balance of what must, should and would be good to be done;

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

d) is traceable and capable of verification;

e) is usable by humans and automated systems;

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

g) addresses all relevant security attributes;

h) manages legacy ICMH Systems;

i) supports compliance with internal and external requirements;

j) is resilient to changes in circumstances, technology and the ICMH System;

NOTE 2 Organizations might well find the need to augment an original scheme, e.g. with additional descriptors, as the role or coverage of an ICMH system evolves. This should not normally mean the ICMH System as a whole needs to change.

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

l) is applied throughout the lifetime and lifecycle of the Information Asset.

The organization shall ensure that its ICMH System is consistent with its overall information and records management policies and procedures as well as compliant with legal and regulatory requirements.

NOTE 3 Users of this British Standard are advised to consider the use of BS ISO 15489-1, BS ISO 55000, BS EN ISO 9001, and BS ISO 30301.

NOTE 4 Attention is drawn to legal and regulatory requirements such as:

- *The Freedom of Information Act [1]*
- *The Freedom of Information (Scotland) Act [2]*

- *The Data Protection Act [3]*
- *The Computer Misuse Act [4]*
- *The Privacy and Electronic Communications (EC Directive) Regulations [5]*
- *The Regulation of Investigatory Powers Act [6]*
- *The Equality Act [7]*
- *The General Data Protection Regulation [8]*

The organization shall define and document that its information handling is suitably integrated with its Information Security Management System (ISMS), where such exists. Where there is no such system in place the integration shall be with the organization's information security policy.

The organization shall consider all opportunities open to it to facilitate effective handling, including simplifying the arrangements as much as possible and supporting them with technology.

NOTE 5 Enforcing features can range from the mandatory use of permanent ink to mark paper documents to the use of digital templates that cannot be changed by users.

6.3 Classification scheme design

6.3.1 Classification criteria

The organization shall document the Classification scheme, detailing how information shall be classified, and by whom, such that people with authorized access to information can understand how it shall be marked and handled.

Information shall be classified according to:

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

b) the risk of inappropriate disclosure, corruption, loss of, or loss of access to, the Information Asset, and the organization's appetite to accept such risk(s);

c) the related costs to the organization of identified risk events occurring and delivering negative impacts such as harm to members of the public, reputation damage, the costs of rectification and of mitigation, etc;

d) the expectations of stakeholders, who might not be directly engaged in the Information Asset, but who nonetheless have the authority to impose requirements eg. legislation and regulation;

e) the need to control the extent of access to the Information Asset throughout its lifecycle;

f) delivering a coherence with, and mapping between, classifications and risk levels used in the organization's risk management process;

g) the amount of assessed effort to protect it;

h) the specific expectations of other organizations with whom Information Assets are shared;

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

The organization shall define and document what action workers shall undertake if they

1) cannot make an assessment of classification; or

2) consider the classification assigned to and marked on an Information Asset to be wrong.

The organization shall consider and document its decision regarding the impact of classification changes on the authenticity and/or integrity of the information.

The organization shall define and document:

i) the procedures to mitigate the impact of classification changes on the authenticity and/or integrity of the information; and

ii) the range and extent of changes to classification that may be performed by workers on each class of Information Asset throughout its lifecycle.

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

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

6.3.2 Hierarchy

Information shall normally be classified according to a hierarchy. The number of classifications in this hierarchy shall be specified by the organization.

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 Annex A.

NOTE 2 The organization should give consideration 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 by the organization.

NOTE 3 An example of a hierarchy might include: highly sensitive; sensitive; not sensitive; and intended for publication.

NOTE 4 These should be meaningful names; for instance, defining access restrictions on a hierarchy of 'not sensitive' to 'highly sensitive' is likely to be more helpful than defining a hierarchy of '1' to '5'.

NOTE 5 If all information were to be classified at the highest level, the efficiency of an organization might be reduced; if all information were to be classified as having no access restriction it is likely this would cause harm to the organization.

Table 1 — *Brief example of a confidentiality hierarchy (informative)*

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 could cause great harm to the organization.
Sensitive	This information is not as sensitive as highly sensitive information but could 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.
Not classified	All other information or Information Assets would be not classified as the information in them would be trivial and access to it poses no danger to the organization.

NOTE 6 A more detailed, example of a hierarchy is given in Table A.1.

6.3.3 Equivalence

When working with a third party involves exchanging or sharing information, the organization shall:

a) explain their ICMH System 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) agree and document the equivalence between the organization's and the third party's schemes whenever possible; and

c) define and document how information that is exchanged or shared will be classified and consequently marked and handled by the third party.

When creating or updating a classification scheme, the organization shall document the equivalence of its ICMH schemes with the schemes of third parties with whom they exchange or share information.

NOTE Consideration should be given to the use of technology to ensure reliable and consistent mapping between these schemes and enforcement of control rules.

6.3.4 Information Asset's lifecycle

The classification scheme shall be continuously applied throughout the Information Asset's lifecycle and shall be managed from creation or capture to eventual disposition, which might be many years later.

NOTE 1 Whilst not directly using the term "lifecycle management" the concept is addressed in more detail in BS ISO 15489-1 where managing records of business activity includes "taking appropriate action to protect their authenticity, reliability, integrity and usability as their business context and requirements for their management change over time".

NOTE 2 It is not uncommon for there to be changes to the classification of specific information, and consequently its marking and handling, throughout the lifecycle of that information in the organization (e.g. from a high degree of control to lower, more relaxed access control).

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

NOTE 3 Changes to classification might 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 organization shall define and document the evidence to be created and retained for planned and unplanned changes in classification of Information Assets.

NOTE 4 An example of the information that might be included in a change log when the classification of an Information Asset changes is as follows:

New classification:

- *date and time of classification/change in classification;*
- *Information Asset classification;*
- *authority for classification change;*
- *classification time, date and any event-related validity (optional); and*
- *anticipated future classification (optional);*

Preceding classification(s) (for each previous classification):

- *date and time of classification change;*
- *authority for classification change;*
- *preceding information classification;*
- *classification validity (expiration) time;*

For any foreseen succeeding classification:

- *trigger for classification change (e.g. time, date, event, etc.);*

- *likely information classification (category, etc.);*
- *authority required for such a classification change;*
- *classification (timeframe) validity (optional).*

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

6.3.5 Default classifications

The organization shall consider whether or not to create and use a default classification and shall document the decisions taken.

NOTE 1 When creating or using a classification scheme, organizations might find it useful to set a default classification that is appropriate for their general, most used, approach to the sensitivity of information as it will normally reduce 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 might be multiple defaults in an organization; for instance, in specific operational units. For example, the default for the Marketing Department might be different from that in HR, where the majority of information is personal and more sensitive than the majority of Marketing's 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.

NOTE 4 When adopting use of a default classification consideration should be given to the balance between user convenience and the awareness and accountability that results from users being required to make a positive choice.

6.3.6 Information Assets that are not marked

Where an organization decides that it shall allow Information Assets to be not marked, and therefore not a specific classification, the organization shall define and document 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.

NOTE 3 This requirement, together with the requirement for training (7.4), is important because recipients of unmarked information might assume it carries no associated handling restrictions and that they have no special duty to restrict access to it.

6.3.7 Descriptors and dependencies

The organization shall specify whether descriptors shall be included within their classification scheme and, if they do so, whether those descriptors shall appear in the marking scheme.

NOTE 1 In some cases it might 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 might be subject to the requirements of UK or EU laws, the requirements of a regulatory body, or the strategic business requirements of the organization.

NOTE 2 The following are examples of possible descriptors:

a) PII: This Information Asset contains personally identifiable information that needs to be protected under EU and UK law.

b) Legal: This is information that EU or UK law requires to be treated 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 EU or UK law.

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 organization shall specify whether dependencies shall be included, or addressed, within their classification scheme and, if they do so, whether those dependencies shall appear in the marking scheme.

NOTE 3 This decision should be based on how likely dependencies are to exist.

NOTE 4 Examples of typical dependencies include:

a) Geography: information may 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 may have different status or significance depending on time and date;

c) Events: a particular event such as a disclosure following a Freedom of Information request, that changes the classification.

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

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

NOTE 5 The organization should consider the number of descriptors and dependencies it needs, if any, and take account of the impact upon its operations that might result from such complexity.

6.4 Marking scheme design

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

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

NOTE 1 For example, headers and footers in electronic documents can be supressed as a default in many document reading or editing programs. A marking scheme using only headers and footers might not always be visible. A mark that depends on a particular program significantly increases the chance that the classification mark will be 'lost' in a change of format.

Where a visible mark is not appropriate, the exception shall be explicitly defined and documented by the organization.

NOTE 2 Except when the Information Asset is for public consumption, having no visible mark should be discouraged.

NOTE 3 Visible is used here as being able to be immediately understood according to the format of the information thus; heard for an audio file, read for a Braille embosser, or displayed on a screen or 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 whilst the new scheme is implemented

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

NOTE 4 Metadata is information many files contain which describes the Information Asset. ICMH technologies and tools commonly use metadata to record and convey classifications. Without the use of such technologies meta data might not be immediately visible and might not automatically get transferred when information changes format.

6.4.2 Placement and style of marking

The organization shall define and document the style, placement and structure to be used for marking Information Assets.

NOTE 1 Style, placement and structure of the mark should be capable of being consistently applied and suitable for the medium or format.

NOTE 2 This British Standard 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 exception shall be defined and documented by the organization.

NOTE 3 Not all information is accessed in a strictly linear fashion (e.g. websites). Where such formats are used, care should be taken that the classification is apparent however it is accessed.

NOTE 4 The marking scheme, while self-consistent, may vary for different classification levels. Information at the least sensitive level of classification should require the least energy or effort in marking, while that at the highest level should be subject to additional effort. For example, highly sensitive information might benefit from continuous marking; marking that is always visible at any point 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 require such complex marking that creators/editors don't attempt to mark it.

The organization shall, wherever possible, automate the application, and prevent the unauthorized deletion, or alteration, of marks on the information.

6.5 Handling scheme design

6.5.1 Handling design criteria

The organization shall define the specific control measures required for each individual classification, to 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.

NOTE 1 For example, such a discrete classification would then form 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.

NOTE 2 For example, the organization might have concluded that encryption of information may be required for some classifications and marks but not others, which should then be made clear to those handling information.

The organization's handling scheme shall explicitly define which individuals can handle the information as well as how they shall handle it.

NOTE 3 The definition of which individuals are entitled to handle information might be by role, by grade or individually as circumstances or organization preferences require.

NOTE 4 When necessary, the suitability of particular individuals should be verified in accordance with the organization's HR policies and procedures. BS ISO/IEC 27001:2013, Annex A provides relevant information.

The organization shall define and document:

a) what automated processing is allowed of marked Information Assets;

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

c) when working versions of Information Assets are to be retained, in what form and for how long; and

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

6.5.2 Information handling during original creation and capture

The organization shall make clear what information can be created and/or captured by which individuals and what approvals are required, and from whom, to do so.

The organization shall ensure that information is classified at the point of creation in accordance with the classification scheme (see **6.3**).

The organization shall define production specifications for all classifications.

NOTE 1 For example, where the asset is a document, these specifications would typically, as a minimum, 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 the Information Asset is another Information Asset type, e.g. an audio or video file, appropriate specifications should be applied.

NOTE 2 If copy numbering is required, it is likely to be to track who the recipients were. In such circumstances the information record would be a sensible place to record this, in addition to in, or on, the Information Asset.

If required for any given classification(s), and then typically for those that relate to particularly sensitive Information Assets, the organization shall maintain a log of the handling of the classification, marking and handling of information throughout the Information Asset's life.

NOTE 3 This will therefore be initiated at first creation i.e. the record is actually the very 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/how the associated marking and handling needs to change.

6.5.3 Information re-use in other Information Assets

The organization shall create and document 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) what permissions and approvals are required; and

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

6.5.4 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 how/if the associated marking and handling needs to change.

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.

6.5.5 Information aggregation

The organization shall define and document how information that is aggregated, or inferred, from other information is then classified, marked and handled.

NOTE 1 Combining information from several sources might result in information with a different classification. The same is true when information is disaggregated. A simple example of when the combination of information from different sources alters the classification, and thus marking and associated handling could be when a list of products *that have been sold is combined with a list of customer names. Furthermore, organizations should be aware 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 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.

6.5.6 Access to information

The organization shall define and apply logical and physical access permissions and controls for the information, based upon the classification. The organization shall define and document how these are granted and managed.

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

The organization 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 rights of a worker to that asset shall be reviewed and the changes documented.

Where required by the organization's ICMH System, and especially its classification and handling schemes, the organization shall ensure that those access rights enable and enforce any limitations set upon the need to know' principle

6.5.7 Information storage

The organization shall define and document the rules for the storage of marked Information Assets.

NOTE 1 Storage rules might 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 may be stored on an encrypted laptop but not on a USB stick, another Information Asset may only be stored on servers within a particular location, while another Information Asset may be stored on public cloud or other sharing platforms.

NOTE 2 For example, whilst marking an electronic document is relatively easy, producing information in audio or video that contains an overlay marking or tone, which cannot subsequently be removed or altered, can be costly.

Systems intended to store and show information in a secure manner might be treated, by default, as denoting that the information is secure. For such circumstances, the organization shall document and communicate that such information can be deemed to have been marked and can be treated as stored securely. Information in such systems shall either be prevented from being extracted or shared; and if it is it shall be marked.

NOTE 3 An example might be that 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 the audio itself should have the security information contained within it.

6.5.8 Information replication and rendering

The organization shall define and document when an Information Asset can be copied, replicated, rendered or otherwise created into a new form. When an Information Asset is replicated or rendered in a different format or media, the classification rules shall stay the same.

The marking and handling rules for the replicated or rendered Information Asset shall follow the ICMH System for the appropriate format or media which might be different from the previous set of rules.

NOTE 1 For example, when an electronic Information Asset is converted, e.g. from a word-processor document format to a PDF, or when the electronic Information Asset is printed, i.e. 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 organization shall define and document the handling rules that shall be applied, including whether or not the replication can take place in an unattended location.

NOTE 2 For example, 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 organization shall define and document whether a record of any replication is required. Where required, the type of record shall be specified and documented.

NOTE 3 The recorded information about replication could 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 in a different physical form the mark style appropriate for the new physical form shall be used.

NOTE 4 For example when an online Information Asset is printed.

The organization shall define and document the instances, if any, in which an Information Asset which has been classified and marked can be reproduced without a classification mark.

NOTE 5 For example, a marketing document might be classified and marked 'Public' during its drafting but the marking would then be dropped upon actual publication, although the handling behaviours would remain in place.

6.5.9 Information redaction

When an Information Asset is redacted, the Information Asset's classification shall be reassessed, and consequently how/if the associated marking and handling needs to change.

NOTE 1 Some Information Assets with appropriate classification can contain information that should not be disclosed to some communities. Modified versions, with differing classification, marking and handling arrangements, should be released to these communities after an appropriate processing of the original. This processing might 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 organization 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 is to be digitally redacted, the processes and procedures used shall ensure that the redacted, removed, information is not recoverable from the redacted Information Asset.

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

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

6.5.10 Information distribution, sharing and exchange

The organization shall make clear 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.

NOTE 1 The handling rights of recipients should include whether they are entitled to further share the Information Asset and how, e.g. whether or not using the 'forward' function that exists in most email systems is allowed.

NOTE 2 Mechanisms, such as secure collaboration platforms, exist to manage this, often supporting the standardised Traffic Light Protocol (TLP) as given in BS ISO/IEC 27010.

The organization 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.

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

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

The organization shall define and document what the precedence arrangements are for its handling scheme versus the handling schemes of any formal sharing or disclosure scheme in which it participates.

NOTE 3 BS 10008 provides useful information in respect of arrangements for legal disclosure and the handling of information that falls in scope of such arrangements.

6.5.11 Information archiving and disposal

In a manner consistent with its overall information and records management policies and procedures, as well as being compliant with legal and regulatory requirements, the organization shall define and document what versions of Information Assets shall be kept, in what form, where and for how long.

The organization shall have policies and procedures for the tracing, capture and disposal of all other copies or versions of Information Assets.

The organization shall define how Information Assets with different classifications, and the media in which they are stored, are deleted, erased or destroyed.

NOTE 1 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 might be considered sufficiently secure for given classifications.

The organization shall define and document how logs and other evidence records of the lifecycle of Information Assets are retained or when and how disposed of.

NOTE 2 BS EN ISO/IEC 27040 and BS ISO 15489-1 both provide useful guidance on archiving and secure disposal of Information Assets.

6.5.12 Information security

The organization shall define and document within its handling scheme, the information security rules to be associated with each classification.

NOTE 1 This might include encryption at rest or in transit, digital rights management, data loss prevention, or secure storage, packaging and carriage rules.

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

NOTE 2 As an example, the hard disk of a laptop might contain information that only the HR Director has permission to access. If the laptop is subsequently used by someone else the rules surrounding the deletion of that information from the laptop , including rules about the method of deletion, should be defined and implemented.

The organization shall define and document within its handling scheme, the encryption rules, if any, to be associated with each classification.

The organization shall define and document within its handling scheme, the encryption rules, if any, to be associated with each classification for information when in transit.

NOTE 3 For example there might 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.

7 Support

7.1 Resources

The organization shall ensure that its ICMH System is sufficiently resourced to enable its success. Such resources shall address all aspects of the ICMH System.

The organization shall ensure that, when resourcing its operations, ICMH is seen as a core activity and not any form of optional activity.

7.2 Roles and responsibilities

The organization shall ensure that the roles and responsibilities of the workers, and their associated access rights and limitations in respect of ICMH, are made explicit and communicated (see 7.3).

The organization shall define and document the ICMH competences required for each identified ICMH role.

The organization shall ensure that, where any automation systems are used in support of ICMH, access rights to those systems are in accordance with, and limited to, the roles and responsibilities assigned to the individuals.

The organization shall define, document and communicate the disciplinary implications of failures to correctly and diligently apply the ICMH System.

7.3 Communication and publicity

The ICMH System itself shall be formally communicated to the organization, and to those with whom it shares information, along with its period of validity and a specified date when it shall be reviewed.

NOTE In addition to providing relevant training (see 7.4), the essence of the ICMH System is often best presented in the form of a table that can then also be provided as a simple, desk-side reference card, poster or similar.

7.4 Training and awareness

The organization shall provide all workers with appropriate and sufficient training in information classification, marking and handling.

NOTE The training provided should cover all of the techniques and technologies involved as well as emphasise that handling is a continuous process throughout the information's life process.

Whether delivered as part of training and awareness or communication and publicity (7.3), the organization shall ensure that suitable information is provided to all workers to enable the organization's ICMH performance to be maintained and enhanced, as appropriate.

7.5 Exercising and rehearsal

The organization shall identify when, or if, any forms of exercising or rehearsal of ICMH practices are required.

NOTE This might be appropriate during the initial deployment of an ICMH System, especially for the more onerous ICMH roles and responsibilities (see 7.2), rather than during on-going training and awareness (see 7.4) or for less onerous roles.

8 Operation

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause **6**, and the improvement actions determined in Clause 9 and Clause 10 by:

a) Establishing the criteria for the required processes, addressing:

   1) System applicability (6.1)

   2) Classification scheme design (6.3)

      i) Classification criteria (6.3.1)

      ii) Hierarchy (6.3.2)

      iii) Equivalence (6.3.3)

      iv) Information Asset lifecycle (6.3.4)

      v) Default classification(s) (6.3.5)

      vi) Unmarked Information Assets (6.3.6)

      vii) Descriptors and dependencies (6.3.7)

   3) Marking scheme design (6.4)

      i) Marking design criteria (6.4.1)

      ii) Placement and style of marking (6.4.2)

   4) Handling scheme design (6.5)

      i) Handling design criteria (6.5.1)

      ii) Information handling during original creation and capture (6.5.2)

      iii) Information re-use in other Information Assets (6.5.3)

      iv) Changes to Information within an existing Information Asset (6.5.4)

      v) Information aggregation (6.5.5)

      vi) Access to information (6.5.6)

vii) Information storage (6.5.7)

viii) Information replication and rendering (6.5.8)

ix) Information redaction (6.5.9)

x) Information distribution, sharing and exchange (6.5.10)

xi) Information archiving and disposal (6.5.11)

xii) Information security (6.5.12)

xiii) reviewing and classifying information received with no marking (6.3.6);

xiv) reviewing and reclassifying information received which is incorrectly classified (6.3.1);

b) implementing the control of the processes in accordance with the criteria;

c) keeping documented information to the extent necessary to have confidence and evidence that the processes have been carried out and planned and;

d) monitoring and treating issues raised by using the approach given in Clause 6.

9 Performance evaluation

9.1 General

The organization shall define an on-going programme of performance evaluation that shall be implemented immediately following the initial implementation of the ICMH System.

The performance evaluation programme shall ensure that:

a) the classification, marking and handling schemes are being operated by all creators 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; and

c) appropriate information is collected to identify deficiencies and facilitate performance improvement (see Clause 10).

9.2 Monitoring and testing

The organization shall define and document the criteria against which the suitability and effectiveness of the ICMH System shall be measured.

The organization shall ensure that there are defined criteria for ensuring and evaluating the compatibility of, and interaction with, different ICMH Systems.

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

NOTE The organization should maintain an agreed assessment of the maturity of its ICMH System(s).

The assessment should cover such considerations as:

a) the degree of coverage of the Information Assets within the ICMH System's scope;

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 ICMH System's goals; and

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

9.3 Auditing and assurance

The organization shall define and document what independent performance evaluation shall be undertaken, if any. This shall be considered alongside self-evaluation of performance that is carried out by those 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.

9.4 Measurement

The organization shall define and document what metrics shall be collected, and , upon the operation of the ICMH System, how frequently and by whom.

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

9.5 Incident management and investigation

In order to support the proper management of information, and facilitate continuous improvement, the organization shall specifically review, and report upon, the ICMH aspects of all security incidents reported to it.

9.6 Reporting and lesson learning

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

The organization shall ensure that this reporting draws out lessons to be learnt and requirements for improvement by, at a minimum, recording causes and deficiencies.

*NOTE Such reporting should encompass all of Clause **9.2** to Clause **9.5** and be designed to facilitate continual improvement (see Clause **10**).*

10 Improvement

10.1 Management review

The organization shall carry out a management review at defined periods. All key ICMH role holders, plus representatives of the ICMH System's operational areas, shall be requested to contribute.

During such management reviews, the organization shall decide what revisions (if any) are required to the ICMH System.

NOTE Examples of topics to be considered during a review are:

a) how the context of the organization might have changed;

b) how the objectives, priorities and activities of the organization might have changed;

*c) the findings of performance evaluation (Clause **9**);*

*d) how existing schemes and Information Assets are dealt with as part of the revision (**10.3**).*

10.2 System revision

Following the periodic management review (see **10.1**), the organization shall ensure 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.

*NOTE To achieve this, the organization should arrange to continuously monitor and maintain its operational context document (see **4.1**) to capture any material changes.*

10.3 Scheme revision

Following the periodic management review (see 10.1), the organization shall ensure 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 organization shall, however, also maintain the capability to make immediate changes to the ICMH schemes if circumstances require it.

NOTE For example, due to change 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, then such changes shall be recorded

10.4 Change management/continuous improvement

The organization shall ensure that it assigns sufficient resources (see 7.1) and allocates roles and responsibilities (see 7.2) to manage changes to the ICMH System and/or subordinate schemes.

The organization shall also assign sufficient resources (see 7.1) along with allocated roles and responsibilities (see 7.2) in order to deliver such continuous improvement to the ICMH system as required.

10.5 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, the organization shall consider developing, documenting and executing a 'roadmap', or similar, for the progressive extension, if any, of the ICMH System.

NOTE There might be some parts of an organization that are perceived to not require any form of ICMH system. The roadmap can be used to recognise and record this. However, it should be assumed that all areas of the organization will have at least a minimum level of requirement for ICMH (using defaults, no marks etc.) such that they fall in scope and can have the ICMH System deployed to them sooner than more complex areas of the organization.

10.6 Progressive integration into the organization

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

NOTE For example:

a) New IT systems might be planned for acquisition that, if selected with the ICMH System in mind, might be capable of more effective enablement of ICMH.

b) New operational processes might be designed to more effectively support ICMH.

10.7 Progressive integration into management systems

The organization shall consider whether to integrate its ICMH System and subordinate schemes into its other management systems.

NOTE 1 Such integration should facilitate the organization's overall efficiency and effectiveness.

NOTE 2 Many management systems (e.g. Information Security, Privacy, Safety, Continuity and Quality) are so intrinsically reliant upon ICMH that the ICMH System design is likely to have been influenced by them at the outset.

NOTE 3 This inter-dependency is likely to require ICMH reporting (see 9.6).

NOTE 4 PAS 99 is a specification for integrated management systems and enables an organization to establish a single framework to manage all of their management systems.

Annex A (informative)
Example Classification, Marking and Handling Schemes

The example schemes given in Table A.1 and Table A.2 are provided solely for illustration of the application of the concepts outlined in this British Standard and not recommended for immediate adoption, although they might be a useful contribution or starting point.

It should be noted that whilst this example uses five levels of classification these are by no means mandatory and might often be excessive.

This example indicates an organization that prioritizes confidentiality over availability or integrity – should those other aspects have been of higher priority the ICMH Schemes would have looked different.

Table A.1 was used by the providing organization as the content for a ‘desktop reminder’ that was provided in the form of a mouse mat and posters.

Table A.2 is the detailed information handling scheme for the providing organization. It expands upon Table A.1 whilst also demonstrating all aspects of this British Standard and of its inter-relationship with the Traffic Light Sharing Protocol (TLP) as defined in ISO IEC 27010:2012.

The approach taken for Table A.2, by the organization that provided this example, was to highlight where there was a requirement only i.e. the absence of specific requirements are not also 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 were 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	Relevant Risk 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 UK economy or political policy. Multi-£m costs and severe embarrassment, making a public response obligatory. Viability of organization and partners threatened.	Strategic plans Passwords Security and Other configurations Credit limits Fraud data Commercial data Corporate policy papers	Recording 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 of c.£1m 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 but less than £100k. 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 Info Meeting minutes Draft public materials	Sharing amongst a group meeting 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

Table A.1 *(continued)*

Classification	Relevant Risk Level	Related Mark	Impact Description	Examples	Essence of Sharing and Handling Rules
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
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*

	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 information record	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 2 factor authentication		Y	Y	Y	
	2 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				

Table A.2 *(continued)*

	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 etc.	Y	Y			
	Chain of custody record	Y				
	Pre-approved sharing platforms		Y			
	Public sharing platforms (e.g. DropBox)			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 / de-gaussed		Y	Y		
	Media physically destroyed	Y				

Annex B (informative) Examples and guidance when applying the ICMH System to Information Assets in different formats and/or media

B.1 Introduction

This annex provides examples and guidance on particular challenges that might 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

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.

B.2.1 Creating paper-based Information Assets

NOTE 1 The creation of a new Information Asset on paper typically requires the use of a blank sheet but it may 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 recorded upon them should be classified and marked (unless default classifications and/or not marked assets are allowed in the ICMH system [see 6.3.5 and 6.3.6]).

b) Information on originally blank paper might 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 6.5).

c) Adding information to a document that is not classified as needing any specific protections might result in a document that does need protection and therefore requires appropriate re-classification, marking and handling.

   NOTE 2 For example a meeting agenda might carry 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 therefore also be handled commensurately.

The organization could consider providing its workers with notepads etc. pre-marked with classifications to focus those workers on the required handling behaviours. However, the organization should consider the practicalities of the proposal to ensure that the benefits are not outweighed by the operational costs.

NOTE 3 For example, carrying several notepads might be inconvenient and onerous, especially if information related to a specific project etc. is also required to be documented separately, which could be signified by a *descriptor or dependency (see 6.3.7). This could 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 record, or by people (such as journalists) who might be 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 might be copied incompletely e.g. without classification marks being copied or with certain pages left out,

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

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

d) the use of printers where these might be in an unsecure location, e.g. workers' homes or public printing services, where adequate data destruction technology might be 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 organization's Handling Scheme should address all stages and states of the lifecycle of a paper-based Information Asset (see especially 6.5.7, 6.5.10 to 6.5.12).

B.3 Electronic documents and digital files

B.3.1 Creating digital Information Assets

In almost all circumstances, the process of creating a digital Information Asset starts with choosing to use a particular software programme. At some point in the creation process, a new file should be created and saved in accordance with the ICMH System (see 6.5.2 to 6.5.5).

B.3.2 Using digital Information Assets

The experience of users of digital Information Assets is affected by the devices and software they use. For instance, the size of their screen or the type and resolution of their web browser affects what a user sees. The organization should therefore assess whether the marking design chosen is adequate under all circumstances. In particular, care should be taken to ensure that:

a) users who access digital files on small screens such as mobile phones are able to see the Information Asset's marking;

b) users who opt for common tools for increasing accessibility such as changing font size, font colour or image size are still always able to see classification markings without having to take a deliberate action such as scrolling sideways;

c) where customization options are available, users are unable to opt out of displaying markings.

As digital files are often easy to manipulate (and thus there is a danger that markings could be deleted or information invisibly altered to change how it should be addressed by the classification, marking and handling scheme), consideration should be given to the following:

1) Certain file formats, such as PDFs, can be used to help preserve information in a particular form. Many file types can be locked against unauthorised textual editing.
2) Digital files can be easy to alter invisibly (in a way that would be impossible with a paper document). For instance, the date, originator or content of an email are all easy to change, such that archiving, with suitable tamper protection, the original document can be an important protection (see 6.5.8, 6.5.9, and 6.5.11 and 6.5.12).
3) It is often possible to 'cut and paste' content from within a document even if it has been protected from editing; in certain circumstances it might be appropriate to consider extra marking(s) within sensitive content (see 6.4.2 and 6.5.3 to 6.5.5).
4) Putting markings in headers and footers in common file formats such as Word and PowerPoint is potentially problematic as a change of template might destroy the headers and footers
5) Markings placed within metadata are likely not to be seen by people using the document.

B.4 Film and tape

B.4.1 Creating audio and video Information Assets

NOTE 1 Most digital Information Assets are documents with a start and an end and with a finite amount of content. These documents can largely be treated in the same way as paper documents with similar markings in accordance with the marking (see 6.4.1). However, not all digital files are page based, some are audio, video or 3D files.

Audio and video assets, whether digitised or on tape or film, are generally relatively straightforward to classify according to the information subject and content plus the participant(s), but are typically more challenging to attach a marking.

In addition to the requirements specified in 6.4, the organization might use the following methods of marking audio and video records within its ICMH System:

a) marking the medium that carries or contains the asset,

   NOTE 2 For example marking the case containing a tape or film.

b) adding the marking prior to the start of the recording so that it is heard or seen before the information asset itself
c) adding the marking at the end of the recording.
d) for audio assets, adding a designated audible tone (unique to a given classification) throughout the recording (although this is likely to impact ability to clearly understand the audio and recognize all its nuances). This means that if a clip of the recording is taken the classification information is still available to anyone who understands the meaning of the tone, as delivered through Training and awareness (see 7.4).
e) for video assets, using a caption, containing the marking, throughout the asset, although care should be taken to ensure that this caption does not then interfere with other caption information such as speech captions
f) using a default classification (see 6.3.5) without marking the individual information asset (see 6.3.6).

NOTE 3 For example, all recordings of telephone calls to a specific call centre would receive the same classification and associated handling arrangements.

g) marking the asset within the metadata associated with the Information Asset, although care should then be exercised, as this might only be appropriate where the rendition of the audio is within a controlled system that recognizes and respects such metadata.

NOTE 4 Some video assets such as public CCTV tapes are likely to fall under data privacy legislation and therefore require a certain level of data classification.

B.4.2 Sharing and transporting tapes and films

Within their ICMH System, organizations might opt for tapes and films classified at certain levels to be subject to specific handling arrangements that are then specific to these media types (see **6.5.10**) that take account of the nature of the media's physical characteristics. As with any other Information Assets, the organization should decide whether certain tape or film assets should not leave the premises.

B.4.3 Storing tapes and films

Tapes and films should have the same consideration applied to their storage as paper assets (see **6.5.7**).

B.5 Voice

B.5.1 Direct conversation

Information that is classified as sensitive should be protected, whenever and wherever it is exposed, including when spoken and especially in the public domain. Someone discussing sensitive information in a public place could be overheard (or even be lip-read) or recorded. Organizations should include in their Handling Scheme how the classification of a conversation is communicated to the participants and the expected limitations on use of the information that is shared. Workers should be made aware of the risks of being overheard.

B.5.2 Communication services

Conversations that are not face to face and make use of telecommunications technology are open to additional risks. Telephones and mobile phones can be intercepted and the conversations recorded. Similarly 'Voice over IP' (VOIP) tools, such as Skype and web based conferencing facilities might not be secure. Organizations might choose to mandate that secure telephony is used for conversations at certain levels of classification.

Organizations should address these issues specifically in the Handling Scheme (see **6.5**) and provide specific training for those workers whose duties most expose them to this risk (see **7.4**).

NOTE Additional information about Sharing Protocols can be found in BS ISO/IEC 27010.

B.6 Images

Many of the considerations discussed in respect of paper, digital, film and audio recording equally apply to image Information Assets.

The organization should ensure that the Handling Scheme makes clear the rules for the original creation of images. The rules should cover resolution, formats, origination attributes (date, time etc.) and the media upon which they can be stored.

Additionally, where images are obtained from third parties, the organization should ensure that the sources are trusted, entitled to the image, that the images themselves can be trusted (not edited or manipulated, suitably current), the most appropriate image for the purpose and of a suitable quality.

Use of the images also requires controls to retain these attributes. The organization should ensure that the handling scheme contains rules for image replication e.g. the production standards/formats used at given classifications to avoid unwanted corruption or abuse.

NOTE The organization might also be required to provide evidence of these attributes e.g. the date and time of original capture.

When handling the image in isolation from, for example, a document in which it might appear, the organization's handling scheme should define whether the marking appears upon it, e.g. as a watermark.

B.7 Mobile working

The ICMH System should address the viewing of Information Assets on mobile devices. It should specify the requirements for screen sizes used, and viewing ability of websites when information is rendered or replicated (see 6.5.8). The organization might choose to mandate within its Handling Scheme that Information Assets classified at certain levels are simply not to be stored or viewed on mobile devices because it is not possible to display the classification marking.

B.8 Assistive technology

The organization should establish with its ICMH System a suitable balance between its potentially conflicting needs to provide support to workers with impairments and information protection.

Software that synthesizes the contents of an Information Asset as sound should include the declaration of the classification and marking.

Presentation of information in braille should do the same and large display and/or character size should not be achieved at the expense of displaying the asset's marking.

B.9 Collaborative platforms

The ICMH System should define what collaboration platforms the organization considers to be public and which private, and which of those are considered secure, e.g. with or without access rights (see 6.5.6, 6.5.10 and 6.5.12).

If the collaboration platform is deemed to be private, then its use should be clearly addressed within the ICMH System. However, if it is deemed to be accessible by the public, the considerations addressed for Social Media (B.12) should be applied. Clearly, collaboration platforms designed for secure exchange of information should be configured to reflect the considerations agreed within the ICMH System to achieve equivalence with that of identified third parties (see 6.3.3).

Where such platforms allow the joint editing of Information Assets, the ICMH System should define which worker reassesses the classification (see 6.5.2 to 6.5.5).

NOTE For example, for efficiency and practicality, this could be done by the last worker to access the Information Asset during a joint editing session or by the defined owner immediately after the editing session concludes. In any event, such a defined owner retains the accountability for the task's execution.

B.10 Database tools

B.10.1 Database access and use

This standard refers to Information Assets as being 'meaningful data', and therefore excludes data held in a database until the point that it is accessed or further processed to create information that can be shared or operated on. This clause therefore refers to information derived from database tools to create Information Assets.

In order to best operate an effective ICMH system, there are particular decisions to be made during:

a) standard database access;

b) ad hoc database extraction; and

c) database manipulation.

B.10.2 Standard database access

Most database systems store information for the software programs an organization uses to support its operations; for example accounting packages, CRM systems etc., and these typically have user access controls (see **6.5.6**). Where it is possible to gain access to the underlying database system, this too should have associated access controls.

Users typically interact with these systems using predefined screens or reports which are a part of the system. These screens and reports, especially if part of a commercially available product, are unlikely to reflect, by default, the classification, marking and handling schemes defined by the ICMH System. Wherever possible, these screens and reports should therefore be adjusted to reflect the ICMH System. Where this is not possible, the ICMH System should communicate the alternative arrangements that users should undertake to manage the associated risks (see **7.3**).

B.10.3 Ad hoc database extraction

The situation described in **B.10.2** is further complicated where information is requested directly from the database, bypassing the standardised screen and reports. For example, database administrators might query the database and create ad hoc lists of information. This information might then be delivered in paper reports, documents or in some human readable digital format such as a spreadsheet. At the point of extracting by the worker performing the extraction or, at least, by the worker who requested the information when receiving it, this new Information Asset should be classified, marked and thereafter handled in accordance with the ICMH System (see also **6.5.3** to **6.5.5**).

B.10.4 Database manipulation

The organization should be aware that Database Management Systems, that bring together numerous databases, as well as 'Data Warehouses' and 'Big Data Solutions', can contain vast amounts of data in seemingly unrelated stores that are called 'tables'.

Access and extraction of information from any single table might contain information with very low sensitivity, however when the tables are joined together in reports etc. or simply when held together, they will typically justify a higher, often much higher, classification (see **6.3.2** and **6.5.5**). Table B.1 shows how joining two tables of data together changes the classification of the data.

Table B.1 — *Example of data manipulation*

Table A		**Table B**	
Name	**ID**	**ID**	**Credit card details**
John	12001	12001	1234-5678-1212
Alice	13222	13222	9876-5432-4545

Workers should therefore make their own assessment of classification, according to the ICMH System, at the point at which they receive the information and not rely on existing systems or information markings as being definitive.

B.11 Websites, internet and intranets

B.11.1 Websites

The ICMH System should be applied to any website(s). Because they are 'non-linear' and comprise collections of Information Assets, consideration should be given in the implementation of the ICMH System's associated schemes and, in particular, marking (see 6.4 and 6.5). Complications could include:

- users have considerable flexibility in how screens are displayed;
- users can select individual parts of a web page for viewing or sharing;
- users might not see information if it is part of a page but not on screen;
- web pages can be dynamically generated, 'on-the-fly' or unique to individual users;
- information on a screen might not actually be displayed metadata, white text, html code etc;
- different browsers and operating systems display information in different ways.

All of these examples mean that there might be more information available than is immediately apparent, which should therefore be presumed by the ICMH System.

B.11.2 Internet

Most internet use can be adequately addressed within the requirements for an ICMH System as covered in this standard. The protocols used in Internet activities such as FTP, WebDAV etc. are simply mechanisms for the exchange of information/Information Assets.

Email should be treated as essentially a mechanism for Information Asset exchange and the ICMH should define methods of marking emails according to their equivalence classification (e.g. in the subject line).

B.11.3 Intranets

In the case of Intranets, in addition to the advice for public websites, Information Assets should be marked according to the ICMH System and access to them managed (see 6.5.6 and 6.5.12).

Each visible screen should be marked according to the highest classification (and associated marking) of all the Information Assets (or parts of them) that are presented (see also 6.5.3 to 6.5.5).

B.12 Social media

By their nature, public social media platforms are essentially open platforms such that information posted upon them can be used and re-used in ways that could well be unacceptable to the organization and the information could remain in the public domain in perpetuity.

Additionally, the organization might not be the originator of all of the information present on its own social media presences. Consequently, the organization should be clear on the limits of permitted handling (e.g. re-tweeting) of others' contributions.

In this instance, the organization should ensure that:

a) the ICMH policy (see 5.4) makes clear to workers what information may or must be published on social media and what penalties will apply if the policy is breached;

b) workers are provided with training and awareness in the Policy requirements (see **7.3**)

c) social media contributions are subject to auditing and assurance (see **9.3**) just as with all the other formats and media discussed in this Annex.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 10008:2014, *Evidential weight and legal admissibility of electronic information — Specification*

BS EN ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

BS EN ISO 9001:2015, *Quality management systems — Requirements*

BS EN ISO 13119:2012, *Health informatics — Clinical knowledge resources — Metadata*

BS ISO 15489-1:2016, *Information and documentation — Records management — Concepts and principles*

BS ISO 30300:2011, *Information and documentation — Management systems for records — Fundamentals and vocabulary*

BS ISO 30301:2011, *Information and documentation — Management systems for records — Requirements*

BS ISO 55000:2014, *Asset management — Overview — Principles and terminology*

BS ISO/IEC 21000-19:2010, *Ed 1, Information technology — Multimedia framework (MPEG-21) — Media Value Chain Ontology*

BS ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

BS ISO/IEC 27010:2012, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

BS ISO/IEC 27038:2014, *Information technology — Security techniques — Specification for digital redaction*

BS EN ISO/IEC 27040, *Information technology — Security techniques — Storage security*

DD ISO/TS 21547:2010, *Health informatics – Security requirements for archiving of electronic health records – Principles*

PD ISO/TR 17797:2014, *Electronic archiving — Selection of digital storage media for long term preservation*

PAS 99:2012, *Specification of common management system requirements as a framework for integration*

Other publications

[1] GREAT BRITAIN. *The Freedom of Information Act. The Stationery Office, London, 2000*

[2] SCOTLAND. *The Freedom of Information (Scotland) Act. The Stationery Office, London, 2002*

[3] GREAT BRITAIN. *The Data Protection Act. The Stationery Office, London, 1998*

[4] GREAT BRITAIN. *The Computer Misuse Act. HMSO, London, 1990*

[5] GREAT BRITAIN. *The Privacy and Electronic Communications (EC Directive) Regulations. The Stationery Office, London, 2003*

[6] GREAT BRITAIN. *The Regulation of Investigatory Powers Act. The Stationery Office, London, 2000*

[7] GREAT BRITAIN. *Equality Act*. *The Stationery Office*, *London*, *2010*

[8] EUROPEAN COMMUNITIES. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal date and on the free movement of such data, and repealing Directive 95/46/EC(The General Data Protection Regulation). Luxembourg: Office for Official Publications of the European Communities.

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.