

BS 10010:2017



BSI Standards Publication

Information classification, marking and handling —

Specification

bsi.

AVA Documents
Document Sharing Hub

Publishing and copyright information

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

© The British Standards Institution 2017

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

	Page
Foreword	iii
Introduction	1
<i>Figure 1 — The ICMH Plan, Do, Check and Act (PDCA) Cycle</i>	2
1 Scope	2
2 Normative references	3
3 Terms and definitions	3
4 Context of the organization	5
4.1 Context and operations	5
4.2 Inter-organizational ICMH co-ordination	5
5 Leadership	5
5.1 Accountability	5
5.2 Setting direction	6
5.3 Leadership and management commitment	6
5.4 ICMH policy	6
5.5 Authority	6
6 Planning and system design	7
6.1 System applicability	7
6.2 Principles	7
6.3 Classification scheme design	8
<i>Table 1 — Brief example of a confidentiality hierarchy (informative)</i>	9
6.4 Marking scheme design	12
6.5 Handling scheme design	13
7 Support	18
7.1 Resources	18
7.2 Roles and responsibilities	18
7.3 Communication and publicity	18
7.4 Training and awareness	19
7.5 Exercising and rehearsal	19
8 Operation	19
9 Performance evaluation	20
9.1 General	20
9.2 Monitoring and testing	20
9.3 Auditing and assurance	21
9.4 Measurement	21
9.5 Incident management and investigation	21
9.6 Reporting and lesson learning	21
10 Improvement	21
10.1 Management review	21
10.2 System revision	21
10.3 Scheme revision	22
10.4 Change management/continuous improvement	22
10.5 Progressive extension of ICMH scope	22
10.6 Progressive integration into the organization	22
10.7 Progressive integration into management systems	22
Annex A (informative) Example Classification, Marking and Handling Schemes	23
<i>Table A.1 — Example Classification and Marking Scheme</i>	24
<i>Table A.2 — Example Handling Scheme</i>	26

Annex B	(informative) Examples and guidance when applying the ICMH System to Information Assets in different formats and/or media	27
	<i>Table B.1 — Example of data manipulation</i>	33
	Bibliography	36

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).

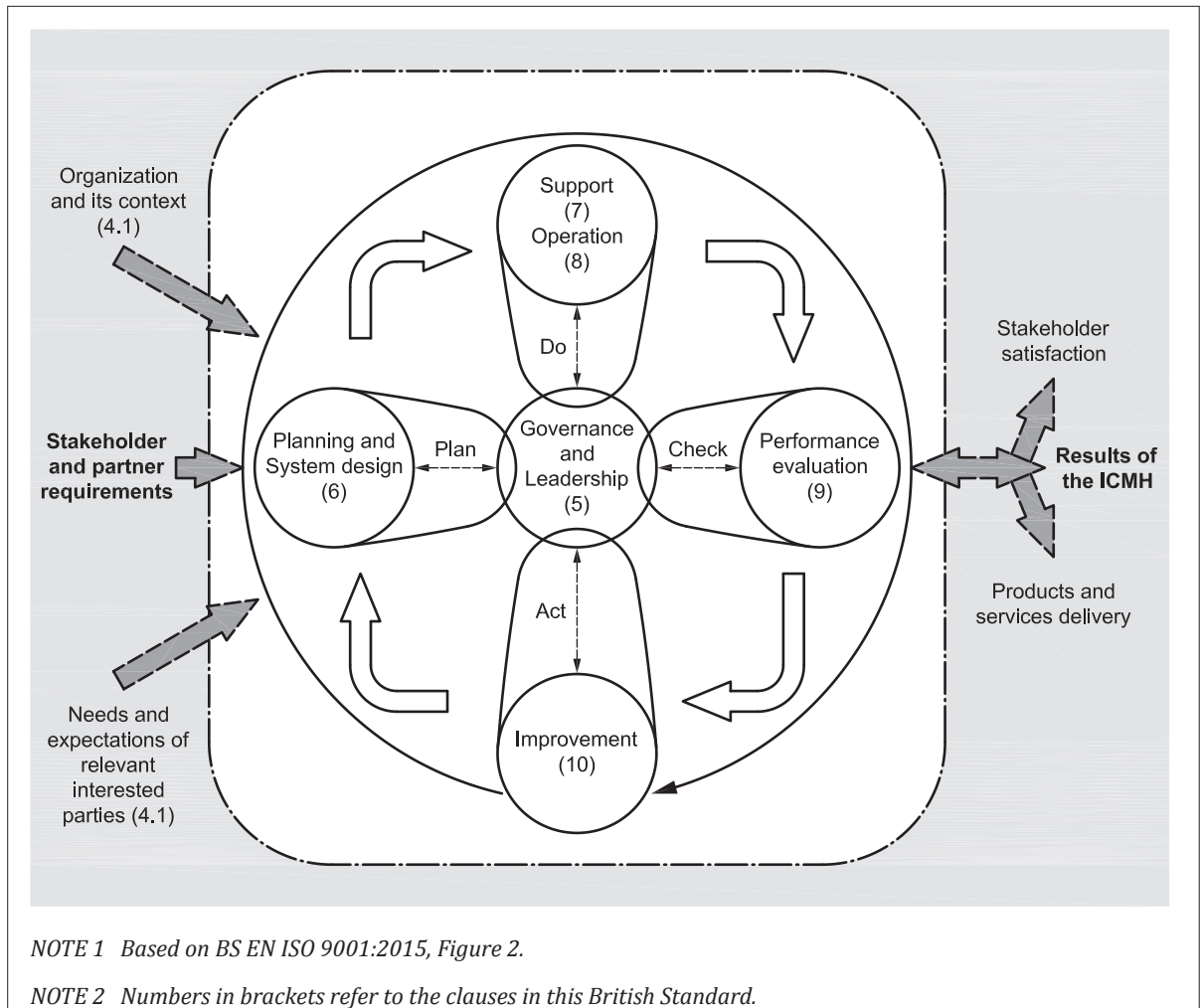
This British Standard intends to encourage organizations, of any size, to use a managed, and more consistent, approach to handling Information Assets on the basis of their classification and marking. This can deliver a significant improvement in how sensitive information is managed, both within the Standard 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



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:

- organizations of any size that create, store, process and/or share information;
- individuals who create, store, process and/or share information;
- individuals with responsibilities for records management, document management, information governance and management, information security, data protection and/or privacy; and
- 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.