

**BS 10008-2:2020**



**BSI Standards Publication**

# **Evidential weight and legal admissibility of electronically stored information (ESI)**

Part 2: Code of practice for implementation of BS 10008-1



**Publishing and copyright information**

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

© The British Standards Institution 2020

Published by BSI Standards Limited 2020

ISBN 978 0 539 05292 3

ICS 03.160; 35.240.30

The following BSI references relate to the work on this document:

Committee reference IDT/1

Draft for comment 19/30390317 DC

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|------|---------------|
|------|---------------|

---

# Contents

|                                                                                  | Page       |
|----------------------------------------------------------------------------------|------------|
| <b>Foreword</b>                                                                  | <b>iii</b> |
| 0 Introduction                                                                   | 1          |
| 0.1 Management summary                                                           | 1          |
| 0.2 Purpose of this British Standard                                             | 1          |
| 0.3 Compliance                                                                   | 2          |
| 0.4 Information as an asset                                                      | 2          |
| 0.5 Technology                                                                   | 3          |
| 0.6 Management framework                                                         | 3          |
| 0.7 Brief history of this British Standard                                       | 3          |
| 1 Scope                                                                          | 3          |
| 2 Normative references                                                           | 4          |
| 3 Terms and definitions                                                          | 4          |
| 4 Context of the organization                                                    | 10         |
| 4.1 General                                                                      | 11         |
| 4.2 Issues                                                                       | 11         |
| <i>Figure 1 — Encryption keys</i>                                                | 14         |
| <i>Figure 2 — Hierarchy of trust</i>                                             | 15         |
| 4.3 Requirements                                                                 | 15         |
| 4.4 Boundaries and applicability                                                 | 15         |
| 5 Leadership                                                                     | 16         |
| 5.1 Leadership and commitment                                                    | 16         |
| 5.2 Policy statements                                                            | 16         |
| 5.3 Roles and responsibilities of workers                                        | 26         |
| 5.4 Legal and regulatory environment                                             | 28         |
| 6 Planning                                                                       | 29         |
| 6.1 Actions to address risks and opportunities                                   | 29         |
| 6.2 Objectives and achievements                                                  | 30         |
| 7 Support                                                                        | 31         |
| 7.1 Resources                                                                    | 31         |
| 7.2 Competence                                                                   | 31         |
| 7.3 Awareness                                                                    | 31         |
| 7.4 Reporting and communication                                                  | 32         |
| 7.5 Documented information                                                       | 32         |
| 8 Operation                                                                      | 42         |
| 8.1 General                                                                      | 42         |
| 8.2 Creation                                                                     | 42         |
| 8.3 Importing                                                                    | 42         |
| 8.4 Business process management, robotic process automation and workflow systems | 45         |
| 8.5 Document scanning                                                            | 46         |
| 8.6 Data extraction                                                              | 47         |
| 8.7 Metadata capture                                                             | 48         |
| 8.8 Self-modifying files                                                         | 49         |
| 8.9 Compound documents                                                           | 49         |
| 8.10 ESI in structured databases                                                 | 50         |
| 8.11 Blockchain and distributed ledger technologies                              | 56         |
| 8.12 Version control                                                             | 56         |
| 8.13 Storage systems                                                             | 59         |
| 8.14 ESI transfer                                                                | 65         |



|                |                                                                   |            |
|----------------|-------------------------------------------------------------------|------------|
|                | <i>Table 1 — Key recommendations</i>                              | 66         |
| 8.15           | Indexing and other metadata                                       | 81         |
| 8.16           | Authenticated output procedures                                   | 82         |
| 8.17           | Identity                                                          | 84         |
| 8.18           | ESI retention, redaction and disposal                             | 101        |
| 8.19           | Information security procedures                                   | 104        |
| 8.20           | System maintenance                                                | 108        |
| 8.21           | External service provision                                        | 108        |
| 8.22           | Information management system testing                             | 115        |
| 9              | Performance evaluation                                            | 115        |
| 9.1            | Monitoring, measurement, analysis and evaluation                  | 115        |
| 9.2            | Internal audit                                                    | 115        |
| 9.3            | Management review                                                 | 117        |
| 10             | Improvement                                                       | 119        |
| 10.1           | Nonconformity and corrective actions                              | 119        |
| 10.2           | Continual improvement                                             | 120        |
| <b>Annex A</b> | (normative) <b>Unstructured message considerations</b>            | <b>122</b> |
| <b>Annex B</b> | (informative) <b>Application of controls</b>                      | <b>128</b> |
|                | <i>Table B.1 — Applicability matrix</i>                           | 130        |
| <b>Annex C</b> | (informative) <b>Example information storage policy statement</b> | <b>133</b> |
| <b>Annex D</b> | (informative) <b>Legal context</b>                                | <b>135</b> |
| <b>Annex E</b> | (normative) <b>Preparation of paper documents</b>                 | <b>141</b> |
|                | <b>Bibliography</b>                                               | <b>157</b> |

### Summary of pages

This document comprises a front cover, and inside front cover, pages i to iv, pages 1 to 160, an inside back cover and a back cover.

---

# Foreword

## Publishing information

This part of BS 10008 is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 30 May 2020. It was prepared by Technical Committee IDT/1, *Document Management Applications*. A list of organizations represented on this committee can be obtained on request to its secretary.

## Relationship with other publications

This part of BS 10008 contains guidance and recommendations for the implementation of BS 10008-1.

## Information about this document

This part of BS 10008 is structured in the same way as BS 10008-1, to assist the reader in locating the appropriate guidance and recommendations when implementing BS 10008-1.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at [bsigroup.com/standards](https://bsigroup.com/standards), or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

## Use of this document

As a code of practice, this part of BS 10008 takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this part of BS 10008 is expected to be able to justify any course of action that deviates from its recommendations.

## Presentational conventions

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

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

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. “organization” rather than “organisation”).

## 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.**



## 0 Introduction

### 0.1 Management summary

It is essential that organizations are aware of the value of the information that they manage, and that they execute their responsibilities under the “duty of care” principle. This British Standard gives detailed guidance on the issues of information management, information security management and requirements to ensure trustworthy information in terms of authenticity and integrity. This part of BS 10008 is arranged, based on and supplements BS 10008-1, and can thus be used as a guide to the implementation of that British Standard.

Information security is significant when discussing evidential weight or legal admissibility issues. Where evidential weight or legal admissibility is being assessed, the main discussion is likely to be related to the authenticity and integrity of the electronically stored information (ESI). When the ESI was captured by the storage system, was the process secure? Was the correct information captured, and was it complete and accurate? During storage since creation or capture, was the information changed in any way, either accidentally or maliciously? When required, is the ESI still available? When responding to these questions, information security implementation and monitoring will be significant evidence when there is a need to demonstrate authenticity and integrity.

### 0.2 Purpose of this British Standard

Users of electronic information management systems are being asked by their companies, government departments and other employers to commit key records and documents under their control to electronic media. The application of these systems is changing the way in which many aspects of business and organizational life are operated, and is creating an electronic legacy for their successors, as paper documents are increasingly replaced by many forms of electronic information storage. Different electronic storage systems and devices have their own inherent advantages and limitations, and existing systems will, at some later stage, be replaced or become obsolete. The purpose of this British Standard is to assist organizations in dealing with the implications, specifically concerning evidential and legal issues, of using technology for their ESI.

This British Standard provides a framework and guidelines based on the requirements of BS 10008-1; it identifies key areas of good practice for the implementation and operation of such electronic storage, transmission and identity management systems, whether or not any information held therein is ever required as evidence in the event of a dispute. As such, compliance with BS 10008-1 can be regarded as a demonstration of responsible business management. This British Standard does not recommend specific technologies – it simply details required attributes, procedures and processes to be applied, together with the requirements for the audit of such systems.

This British Standard also covers the application of technology to provide electronic message sender and recipient identity verification; this is the association of identity with transferred ESI and linking identity of copyright ownership to ESI. These might be by the use of digital signatures; where similar or associated cryptographic techniques are also used for confidentiality, this application is addressed in this British Standard. [Annex A](#) gives further details of procedures that are applicable to unstructured messaging systems.

This British Standard does not cover the application of identity and identity tokens for access to services. These logical and physical access control functions might well use techniques in common with those used in this British Standard. The fundamental question asked when an identity is attributed to an individual (e.g. proof of identity) is a common issue that needs to be addressed.

In order to provide widely applicable guidance, this British Standard does not recommend system hardware or software configurations, and thus is technology independent.

[Annex B](#) gives details of specific applications that can be managed under the control of this British Standard.

### 0.3 Compliance

BIP 0009, a Compliance Checklist [1] is a companion to BS 10008-1 and this British Standard. This checklist enables a comprehensive assessment to be made of the user's information management system for compliance with BS 10008-1. Completion of a copy of the Compliance Checklist for each system and associated storage and retrieval processes provides one means of satisfying key elements of the audit trail.

Where compliance on a self-assessment basis is claimed, recommended compliance statements to use are given in [9.3.4](#), which also includes further information on compliance audits.

Where compliance is assessed by a third party, liability for compliance will normally remain the responsibility of the organization. Compliance with BS 10008-1 does not guarantee evidential weight or legal admissibility. Information that is stored or transferred using systems not in conformance to BS 10008-1 might be legally admissible and can be assessed for evidential weight, but it might be more difficult to demonstrate information authenticity and integrity in the event of a dispute than if the system was in conformance to BS 10008-1.

### 0.4 Information as an asset

The top management of any organization is responsible for the conduct of that organization in every way – financially, operationally, legally and ethically. Specifically, it has responsibility for its assets and their use. Many responsibilities of top management concern the activities and processes of the organization, for example, investment for a new product, selling in a new market or building a new plant. However, some of the most important responsibilities are defined functionally by subject, for example, financial affairs and human resources. One such subject is information – not information systems but the stored information itself.<sup>1)</sup>

Organizations operate by producing, transmitting and digesting information. The right information at the right place at the right time is essential for effective conduct of business. Equally, the misuse, copying, theft, loss and abuse of information can be, and have very publicly been, the cause of scandals and business failures.

Information is required in every activity and every function, thus proper control of information and care in its use have always been a subject of concern. Modern computers and communications systems can store information, process it and make it accessible in ways never before achieved. This can be of great additional benefit to business but can also enhance opportunities for misuse, theft, loss and abuse and, in particular, indiscriminate dissemination of information.

In some organizations, it is accepted that some types of business information are assets, for example, customer and services information and intellectual property such as patents and copyright. All information in an organization, regardless of its purpose, needs to be properly identified, even if identification is not required for accounting purposes, for consideration as an asset of the business. Conversely, retaining ESI beyond its required retention period can be a business liability, for example, an increased cost of storage, or a breach of statutory requirements, for example, regarding the processing of personal information.

<sup>1)</sup> The 1995 report "*Information as an Asset*" [2], produced by the Hawley Committee with the support of the KPMG IMPACT team, has been updated (February 2019) to encourage a new generation of top management to engage with the strategic value of the information assets in their organizations.

## 0.5 Technology

It is important to utilize reliable and trustworthy technology to manage ESI over a long period of time, potentially with the implementation of replacement technologies. Each part of the system needs to be chosen with care, taking into account the possible need to demonstrate “proper” and “appropriate” working of the system sometime in the future. This demonstration might need to encompass both the technology itself and the methods by which it was configured and used. The technology sections cover particular aspects of technology (e.g. the storage media used) as well as critical aspects of configuration (e.g. how access to the system is managed).

## 0.6 Management framework

BS 10008-1:2020, Clause 1 to Clause 7, are structured along the lines of the standardized structure of the ISO Management System Standards, such that its implementation can be synchronized with other management systems, such as BS ISO/IEC 27001, where appropriate.

## 0.7 Brief history of this British Standard

BSI originally published a Code of Practice for Evidential Weight and Legal Admissibility in 1996.

This was supplanted by a British Standard, BS 10008, in 2008 (and updated in 2014), reflecting requests of the adopters of the original code of practice for a formal compliance standard.

However, it was recognized that the standard lacked detailed implementation guidance and therefore the standard was complemented with three further BSI publications to address the various sections of the British Standard:

BIP 0008-1, *Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008* [3];

BIP 0008-2, *Evidential weight and legal admissibility of information transferred electronically – Code of practice for the implementation of BS 10008* [4]; and

BIP 0008-3, *Evidential weight and legal admissibility of linking electronic identity to documents – Code of practice for the implementation of BS 10008* [5].

To accompany the latest revision of BS 10008-1:2020, these three separate documents have been consolidated into this British Standard, BS 10008-2.

---

# 1 Scope

This British Standard gives recommendations and guidance for the implementation and operation of information management systems that manage information electronically (including where the electronic information is transferred from one computer system to another) and where the issues of authenticity, integrity and availability as required for legal admissibility and evidential weight are important. It describes the processes for use in the identification and development of policies and procedures as specified in BS 10008-1, in relation to the management of electronically stored information (ESI).

This British Standard is applicable to any system that:

- a) stores and/or transmits information electronically;
- b) uses any type of database or other electronic system; and/or
- c) manages information electronically, using any type of electronic storage medium including write-once-read-many (WORM) and rewritable technologies.

This British Standard also covers procedures and processes relevant to the following ESI authentication principles:

- 1) electronic identity verification – proving the genuineness of the individual/organization that produced, transferred and/or stored the electronic document;
- 2) electronic signature – the application of the legal equivalent of a “pen and ink” signature on a paper document;
- 3) electronic copyright – the application of a copyright mark to ESI; and
- 4) linking the electronic identity and/or electronic signature and/or electronic copyright to the particular ESI (and preventing compromise to its integrity).

It covers aspects of the information management processes that affect the use of ESI in normal business transactions, even where legal admissibility per se is not an issue. Such aspects include the legibility, accuracy and completeness of the ESI, and the transfer of the ESI to other systems.

This British Standard is also applicable to electronic identity management systems and can be applied to any form of electronic identity management system, irrespective of the technology used.

This British Standard is intended for:

- end user organizations that wish to ensure that ESI captured by, imported into, stored and/or transmitted within their information management systems can be used with confidence as evidence in any dispute, within or outside a court of law;
- end user organizations that wish to ensure that electronic identity management systems can be used with confidence as evidence in any dispute, within or outside a court of law; and
- integrators and developers of information management systems that provide facilities to meet user requirements.

This British Standard does not cover processes used to evaluate the authenticity of ESI prior to it being imported into the system. However, it can be used to demonstrate that output from the information management system is a true record of what was imported.

Compliance with this British Standard does not guarantee legal admissibility. It defines good practice.

---

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application<sup>2)</sup>. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 10008-1:2020, *Evidential weight and legal admissibility of electronically stored information (ESI) – Part 1: Specification*

BS ISO 12651-1, *Electronic document management – Vocabulary – Part 1: Electronic document imaging*

---

## 3 Terms and definitions

For the purposes of this part of BS 10008, the terms and definitions given in BS 10008-1, BS ISO 12651-1 and the following apply.

---

<sup>2)</sup> Documents that are referred to solely in an informative manner are listed in the Bibliography.

### 3.1 audit

systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

*NOTE 1 An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).*

*NOTE 2 "Audit evidence" and "audit criteria" are defined in BS EN ISO 19011.*

[SOURCE: BS EN ISO 9000:2015, 3.13.1, modified – Note changed]

### 3.2 audit trail

data that allow the reconstruction of a previous activity, in its correct chronological place, or which enables the attributes of a change (such as date/time or operator) to be recorded

*NOTE The list can be generated by a computer system (for computer system transactions) or manually (usually for manual activities).*

### 3.3 audit trail data

information stored in the audit trail

### 3.4 authenticity

property that an entity is what it claims to be

[SOURCE: BS EN ISO/IEC 27000:2020, 3.6]

### 3.5 availability

property of being accessible and usable upon demand by an authorized entity

[SOURCE: BS EN ISO/IEC 27000:2020, 3.7]

### 3.6 bitmap

digital image where each pixel is represented by one bit, representing black or white

### 3.7 black border removal

removal of contiguous areas of black pixels that surround the edges of document images, and which have been created by a scanning process

### 3.8 cloud

model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction

[SOURCE: NIST Special Publication 800-145, "The NIST Definition of Cloud Computing" [6]]

### 3.9 compliance

conforming to a rule; such as a specification, policy, standard or law

### 3.10 data

series of digital or analogue signals or encoded characters stored or transmitted electronically, or marks (e.g. writing, printed characters or graphics) on paper or microform, that are intended to convey information

*NOTE The essential distinction between data and information is that data do not need to have any meaning attached to them. Data become information via context; the same data file (see 3.11) might be considered as containing different information depending on the context: the data in the same file might be considered as*

*containing ASCII characters as far as one computer program is concerned; another might regard the same data as a set of names and addresses; the user might know that these are customer names and addresses.*

### 3.11 data file

related data handled as a discrete unit

### 3.12 data record

item of data in a specified format as part of a data file

### 3.13 database

- a) collection of interrelated data stored together in one or more computerized files
- b) collection of data organized according to a conceptual structure describing the characteristics of the data and the relationships among their corresponding entities, supporting one or more application areas
- c) collection of data describing a specific target area that is used and updated by one or more applications

[SOURCE: BS ISO/IEC/IEEE 24765:2017, 3.1042]

### 3.14 database management system (DBMS)

software system designed for the definition, creation, querying, update and administration of databases

### 3.15 digital image

image consisting of pixels using ranges of discrete values

### 3.16 digital signature

data appended to a data file that allow the recipient of the data file to authenticate the source and the integrity of the data file

*NOTE 1 A digital signature can also store the date and/or time of signing.*

*NOTE 2 A digital signature can also be used to demonstrate that the data file could have originated only from the purported sender.*

### 3.17 dpi

dots per inch, a measure of resolution

### 3.18 electronic signature

data which, when appended to a digital document, enable the user of the document to authenticate its origin and integrity

[SOURCE: BS ISO 20415:2019, 3.6]

### 3.19 electronic storage

storage medium or device used by an information management system to store information

*NOTE Electronic storage specifically includes magnetic disks, magnetic tapes, storage area networks (SANs), network attached storage (NAS), hierarchical storage management (HSM) systems and optical disks of all sorts.*

### 3.20 encryption

reversible process of converting a data file into a secret code under the control of a key

**3.21 expungement**

process of removing a document from a system and leaving no evidence of the document ever having appeared on the system

**3.22 file**

<computerized data> see “data file”, [3.11](#)

**3.23 file**

<microform media> microfilm rolls or sets of microfiche or film jackets contained within a single envelope

**3.24 file**

<paper> devices for holding documents, including inter alia, envelopes, box files and ring or other types of binder

**3.25 forms removal**

system (usually software) which removes a “fixed” overlay from a digital image, leaving only the variable data

**3.26 frozen**

defines a specific point in time at which no change to the contents of a specified data file is subsequently permitted to occur

*NOTE This is a fundamental concept in this British Standard. After a file has been “frozen”, any copies made of this file should contain exactly the same data.*

**3.27 governance**

process of establishing and enforcing strategic goals and objectives, organizational policies and performance parameters

[SOURCE: BS ISO/IEC/IEEE 21841:2019, 3.1.2]

**3.28 greyscale image**

image formed of picture elements (pixels) containing greyscale information

**3.29 hierarchical storage management (HSM)**

data storage technique that involves using a number of electronic storage devices, from fast access to slow access, within which data files can be moved under system control from one device to another

**3.30 hierarchical storage system**

data file storage system using a number of electronic storage devices, from fast access to slow access, within which data files can be moved under system control from one device to another

*NOTE Storage devices can range from high cost, fast access devices to low cost, slow access devices. They are used to optimize the performance and cost characteristics of the storage and retrieval system.*

**3.31 information**

data interpreted in an application context (see also [3.10](#))

*NOTE For example, a string of characters may be referred to generally as data; but if these characters are understood by a person or a computer program as someone’s name, then the characters convey information. Information always involves the presence of data in some format, on some medium, which could be, for example, a physical document, a document image on a screen or the contents of an electronic file.*

### 3.32 intelligent character recognition (ICR)

advanced optical character recognition (OCR), or rather more specifically, hand-printed recognition system that allows fonts and different styles of handwriting to be learned by a computer during processing to improve accuracy and recognition levels

[SOURCE: ISO 12029:2010, 3.5]

### 3.33 key escrow service

function provided by an organization to keep secure copies of encryption keys, in a manner that requires consent from the key owner before the key is disclosed

### 3.34 lossless compression

data file compression technique where the decompressed image is identical to the original uncompressed image

*NOTE No information is lost during the compression and decompression process.*

### 3.35 master data management (MDM)

policies, processes, tools and governance to consistently define and manage significant data of an organization and to provide a single point of reference for that data

### 3.36 multi-functional drive system

optical disk drive which can use both write-once read-many and rewritable optical media

### 3.37 network attached storage (NAS)

server that is dedicated to nothing more than file sharing

*NOTE NAS does not provide any of the activities that a server in a server-centric system typically provides, such as email, authentication or file management.*

### 3.38 NoSQL

database providing a mechanism for storage and retrieval of data that can be modelled in means other than the tabular relationships used in relational databases

*NOTE 1 The term NoSQL is short for "Not only SQL" in that SQL-like query languages can be supported in addition to other methods.*

*NOTE 2 Many NoSQL databases lack full ACID transaction support.*

### 3.39 objective

result to be achieved

*NOTE 1 An objective can be strategic, tactical or operational.*

*NOTE 2 Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).*

*NOTE 3 An objective can be expressed in other ways, for example as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g. aim, goal or target).*

*NOTE 4 In the context of information security management systems, information security objectives are set by the organization, consistent with the information security policy, to achieve specific results.*

[SOURCE: BS EN ISO/IEC 27000:2020, 3.49]

**3.40 optical character recognition (OCR)**

technique for the recognition of characters from a digital image

*NOTE Identification of vehicles using Automatic Number Plate Recognition (ANPR) systems for law enforcement, tolls, parking enforcement, etc. is an application of OCR.*

**3.41 optical disk**

disk that will accept and retain information in the form of marks in a recording layer that can be read with an optical beam

**3.42 optical mark recognition (OMR)**

technique for electronic detection of marks in specified locations on a digital image

**3.43 original document**

document from which a copy is made or from which an image is captured

**3.44 outsource**

make an arrangement where an external organization performs part of an organization's function or process

*NOTE 1 This often includes a transfer of workers to the third party.*

*NOTE 2 An external organization is outside the scope of the management system, although the outsourced function or process is within the scope.*

[SOURCE: BS EN ISO/IEC 27000:2020, 3.51]

**3.45 page**

single image entity

*NOTE For example, one side of a sheet of paper, a drawing or plan, map, photograph, transparency; or a microform "frame".*

**3.46 pixel**

smallest two-dimensional element of a digital image that can independently be assigned attributes such as colour and intensity

*NOTE The word is derived from "picture element".*

**3.47 records management**

field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records

[SOURCE: BS ISO 15489-1:2016, 3.15]

**3.48 resolution**

ability of a scanner or image generation device to reproduce the details of an image

**3.49 scanning**

operation that converts the image of a document into a digital form, by detecting the amount of light reflected from elements of the document

### 3.50 schema

logical plan showing the relationships between metadata elements

*NOTE The relationships are normally through establishing rules for the use and management of metadata specifically as regards the semantics, the syntax and the optionality (obligation level) of values.*

[SOURCE: BS ISO 23081-1:2017, 3.10, modified]

### 3.51 skew

poor document alignment (rotation) during scanning

### 3.52 speckle

random, or quasi-random, black marks (speckles) on an image, either generated during the scanning process, or present on the original document

### 3.53 storage area network (SAN)

sub-network (typically high speed) of shared storage devices

*NOTE A storage device is a machine that contains nothing but a disk or disks for storing data and the necessary control mechanisms for storing that data. A SAN's architecture works in a way that makes all storage devices available to all servers on a local area network (LAN) or a wide area network (WAN).*

### 3.54 system files

files held in a computer for use in the control and operation of the system

### 3.55 trusted time

time stamping of ESI performed by, or with the direct involvement of, a party underwriting the accuracy and consistency of that time stamp

*NOTE 1 Trusted time is time that is certified to be traceable to the time source for the application in which it is being used and is not forgeable either at the time of initial use or anytime in the future.*

*NOTE 2 Trusted time stamps are used to enhance the integrity or authenticity of ESI to which they relate. They are often used in conjunction with cryptographic digital signatures.*

### 3.56 workflow

automation of a business process, in whole or in part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules

[SOURCE: Workflow Management Coalition Specification, *Terminology and Glossary*, WPMC-TC-1011 [7]]

### 3.57 write-once-read-many (WORM)

form of electronic storage medium that permits data to be stored once, read many times, but not altered

---

## 4 Context of the organization

### COMMENTARY ON CLAUSE 4

*This clause of this British Standard relates to BS 10008-1:2020, Clause 4.*

*Everything in an organization involves using electronically stored information (ESI) in some way. The quantity of ESI can be vast, and there are many different ways of representing and storing it.*

## 4.1 General

In order to ensure that ESI is well managed, and to meet its business needs, the organization should define and implement good management practices. ESI, like any other asset, should be classified, structured, validated, valued, secured, monitored, measured, managed and disposed of, when appropriate, efficiently and effectively.

All ESI used by an organization should be classified into “information types”. This classification should be used in the creation of a “policy statements” which extends to accommodate the transferred ESI covered in this British Standard.

Increasingly, ESI is being sent from one electronic system to another, either within an organization or between organizations. The manner in which this movement of ESI occurs can determine the success or failure of the organization; thus, transfer systems should be secure, structured and auditable.

*NOTE 1 Where information is received electronically from another organization, knowledge of the processes used to transfer the ESI is key to a successful, legally admissible electronic transfer system.*

*NOTE 2 When defining a transfer policy, the relative importance of speed of delivery, both to the recipient organization and to the recipient in that organization, might be significant. Taking two extremes, direct transfer to a PC across the internet or via a carrier usually results in almost instantaneous transfer, whereas transfer by post can be measured in days.*

*NOTE 3 With the move from paper originals to electronic original documents, the use of the electronic equivalent of an ink signature becomes an important part of a document authorization process. A signature can also be used as a method for authenticating the contents of a document.*

*NOTE 4 Technologies can be implemented that apply electronic signatures of various forms to electronic documents, with various degrees of confidence and integrity. Some systems also allow for the verification of an electronic signature by another individual or organization [a trusted third party (TTP)].*

As with many types of electronic systems, however, simply implementing technology might not provide the weight of evidence necessary should an electronic identity be challenged. Appropriate policies and procedures should be implemented in order to create secure, structured and auditable electronic identity management systems.

## 4.2 Issues

### 4.2.1 General

The organization should determine the external and internal issues that are relevant to its purpose and that might affect the authenticity and integrity of the ESI that it uses and transfers.

*NOTE 1 Typical issues that might be relevant include:*

- a) the size and complexity of the organization;*
- b) the level of business risk attached to being unable to demonstrate authenticity and integrity of ESI;*
- c) drivers for business efficiency improvements;*
- d) specific stakeholder requirements; and*
- e) the existing technology and infrastructure systems.*

Policy statements as described in [5.2](#) should take into account those issues that are agreed to be relevant to the ability to demonstrate authenticity and integrity of ESI.

*NOTE 2 When reviewing the relevant issues, a risk management process is the most appropriate to use when deciding upon actions to be undertaken. BS ISO 31000 provides principles, framework and a process for managing risk. PD ISO/TR 18128 gives further advice on risk assessment in relation to records management. It can be used by any organization regardless of its size, activity or sector. Using BS ISO 31000 can help organizations increase the*

*likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.*

*NOTE 3 The requirement to authenticate ESI assets that have evidential significance to an organization might be vital to continued operations. Such authentication systems are becoming more widespread, and various features have been established by organizations involved with these systems. Authentication in this British Standard deals with proof of identity in relation to document signatories, and to copyright issues.*

#### 4.2.2 Electronic and digital signatures

*NOTE 1 The terms electronic signature and digital signature are often used interchangeably but they are not the same and the law, in most jurisdictions, goes to some length to clearly distinguish between them.*

*NOTE 2 There are many forms of electronic signature, many of which are not particularly resistant to fraud, although fraud is also prevalent with handwritten “wet” signatures. Electronic signatures have many of the same problems as handwritten signatures but also have some others to consider.*

Digital signatures created using current cryptographic methods, algorithms and key strengths might not be sufficiently secure in the future. Consequently, the organization should document digital signature algorithms and keys utilized.

The organization should also plan how to address content digitally signed when current methods, algorithms and key strengths are, or are expected to be, superseded.

*NOTE 3 The Law Commission report on Electronic Execution of Documents [8] clarifies the validity in English law of electronic signatures and makes clear that different types of electronic signature have different strengths and that the weaker types (e.g. a scanned image of a handwritten signature, typed name in an email, etc.) might not be appropriate for higher value/risk content.*

At the planning stage, appropriate third parties who will need to use or inspect the results from authentication systems as detailed in this British Standard should be consulted.

*NOTE 4 Examples of such third parties are:*

- a) receiving parties;*
- b) auditors;*
- c) legal experts; and*
- d) technical and operational staff.*

*NOTE 5 The requirement to verify digital or electronic signatures or other identification systems of ESI by third parties, with full legal significance, is far-reaching. Such verification systems based on digital certificates are becoming more frequently required as an independent check on ESI integrity, origination, authority and authenticity. Similarly, the successful use of copyright protection systems can be critical to the success of an organization.*

Organizations that provide independent verification services (TTPs) should be consulted when designing and implementing procedures for the verification of such systems in the event of a challenge from another organization.

Different organizations might not use the same trusted third party (TTP). Where this situation occurs, the procedures for the various TTPs might be different, as might the services offered, the rigour of checks performed and liabilities accepted. Therefore, procedures should be strictly controlled under these circumstances.

The user of a specific TTP should be aware of the “network of trust” that their TTP is a part of, and should ensure that its liability for certificate verification is handled by its TTP (and not “passed on” along the chain to a less trustworthy organization).

### 4.2.3 Encryption keys

A digital signature uses a pair of cryptographic keys; one of these keys is Private and the other is Public. The Public Key is shared but the Private Key should be retained securely.

*NOTE 1 If someone else has access to an individual's Private Key then they can fraudulently digitally sign for that individual as an imposter. This is why security of the Private Key is critical to the robustness and trustworthiness of something digitally signed. See [8.14.2.7.2](#).*

*The two important attributes of digitally signed ESI are that:*

- *the signer is the person with the Private Key; and*
- *what was signed has not been changed since the act of signing.*

*NOTE 2 Software, usually on a user's computer, generates the pair of encryption keys that will be used in secured applications – a Public and a Private Key.*

The Private Key should never be distributed or revealed; conversely, the Public Key can be freely distributed to any party that negotiates a secure transfer.

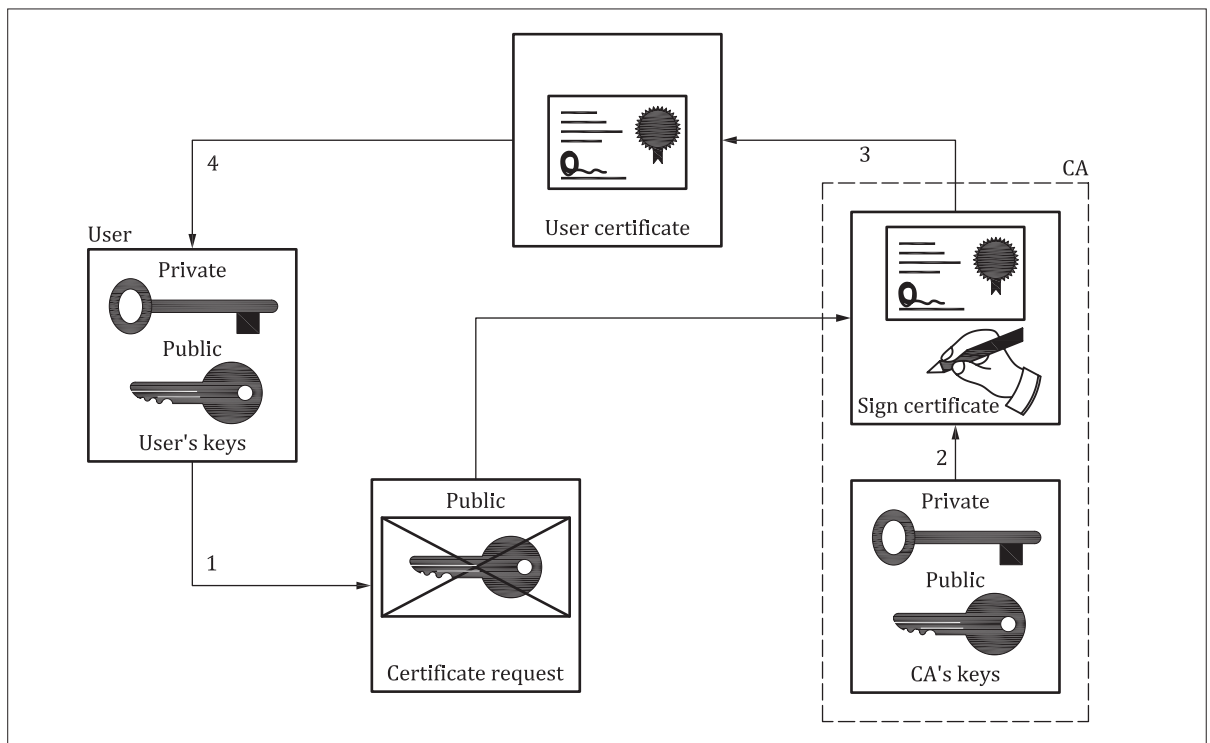
During the registration or enrolment process, the user's Public Key should be sent in a certificate request to the certification authority (CA) or its authorized agent, a registration authority.

*NOTE 3 When the CA approves the request, it generates the user's digital certificate. The user's certificate will have been digitally signed by the CA. After the user receives their certificate and installs it on a computer, they can participate in the secured application.*

*NOTE 4 The user's digital certificate (an X.509 certificate) contains the user's Public Key and has been digitally signed by the CA after checking that the user really is who they purport to be. This can be to different levels of confidence depending on how the checks are conducted.*

*NOTE 5 The digital certificate is then used either for encryption or digitally signing (frequently there will be two sets of keys and two certificates; one for encryption and a separate one for digital signing). The digital certificate, containing the user's Public Key, is used by someone wishing to encrypt data for that user; the user decrypts those data using their Private Key.*

For digital signing, the user's Private Key should be used, and the Public Key (in the certificate) is then able to confirm the integrity of the signed content and that it was signed by the user, whose identity was confirmed by the CA before they signed the user's certificate. See [Figure 1](#).

**Figure 1** — Encryption keys

#### 4.2.4 Hierarchy of trust

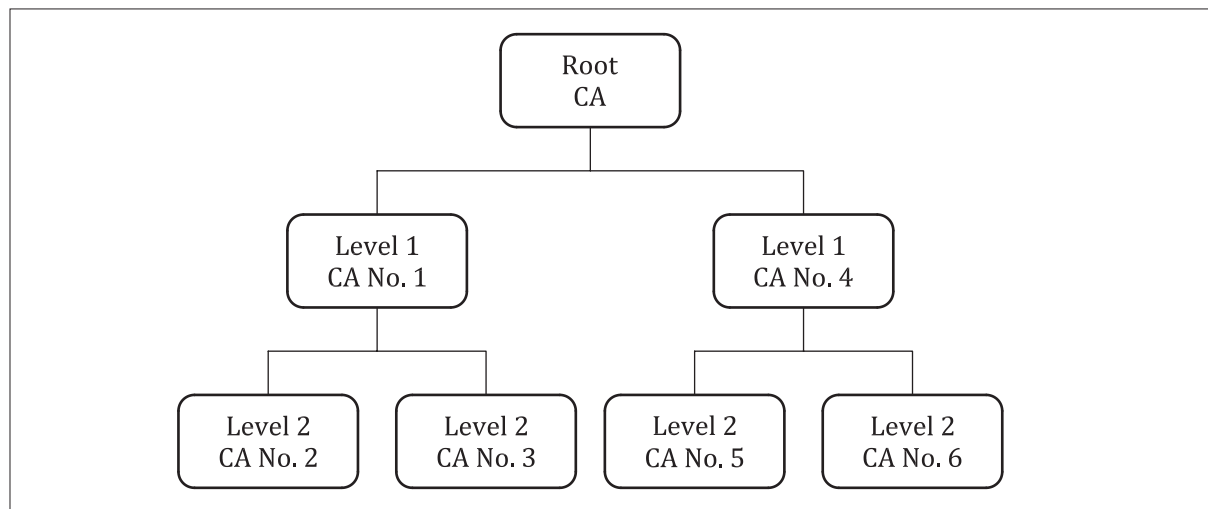
There is a concept of hierarchy of trust; this is simply that there should be a certification authority (CA) that everyone agrees is trustworthy.

*NOTE 1* This ultimate authority is called the root CA. The root authority can then certify other CAs below it, which can then certify CAs below them, etc. This is illustrated in [Figure 2](#).

*NOTE 2* When a certificate is received that has been issued by a first or second level CA, the user can verify that the CA that signed the certificate has been certified by a CA at the level above it and, in turn, that CA has been certified by the one above that, and so on until a chain of trust exists between the lower level CA (or a user certificate) and the root CA. For example, in [Figure 2](#), it can be verified that CA No. 3 was certified by CA No. 1, and that CA No. 1 was certified by the root CA.

When a certificate from a lower level CA is passed along with an encrypted message, all of the certificates in its chain of trust up to the root should be passed along with it.

The organization, therefore, should ensure that the agreements between the members of the network of TTPs are adequate to deliver the required verification service and that the fiscal guarantees in the event of failure are sufficient to meet its requirements.

**Figure 2** — *Hierarchy of trust*

### 4.3 Requirements

When establishing or reviewing the systems and/or processes that manage the evidential weight of ESI, the organization should determine:

- stakeholders that are relevant to the authenticity and integrity of ESI;
- the requirements of these stakeholders relevant to that ESI; and
- the requirements for information stewardship within the organization.

*NOTE The requirements of stakeholders might include legal and regulatory requirements and contractual obligations.*

*Typical stakeholders might include:*

- owners, managers and staff of the organization;
- third parties with contracts or similar agreements with the organization;
- clients and customers in receipt of services provided by the organization;
- the public where public services are involved;
- regulatory bodies;
- government bodies;
- external audit bodies; and
- legal advisers.

The requirements of each stakeholder should be taken into consideration when producing policy statements (see 5.2).

Information stewardship should be managed by the identification of Information Asset Owners (IAOs) who are typically those responsible for the processes that generate the ESI asset in question.

### 4.4 Boundaries and applicability

The organization should determine the boundaries and applicability of the authenticity and integrity of the ESI it uses in order to establish its scope.

When determining this scope, the organization should consider:

- the external and internal issues referred to in 4.2;
- the requirements referred to in 4.3; and

- c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope should be available as part of the policy statements.

In many organizations, the authenticity and integrity of ESI will only be of importance to part of the overall ESI asset. As part of a project to implement BS 10008-1 and this British Standard, individual ESI assets should be identified and a decision should be taken as to whether each is to be included within the scope of the related policy.

---

## 5 Leadership

### COMMENTARY ON CLAUSE 5

*This clause of this British Standard relates to BS 10008-1:2020, Clause 5.*

### 5.1 Leadership and commitment

Top management should demonstrate leadership and commitment with respect to the management of the ESI authenticity and integrity by:

- a) ensuring the information management policies and objectives are established and are compatible with the strategic direction of the organization;
- b) ensuring the integration of the information management system requirements into the processes of the organization;
- c) ensuring that the resources needed for the information management system are available;
- d) communicating the importance of effective information management and of conforming to the information management system requirements;
- e) ensuring that the information management system achieves its intended outcome(s);
- f) directing and supporting persons to contribute to the effectiveness of the information management system;
- g) promoting continual improvement; and
- h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

### 5.2 Policy statements

#### 5.2.1 General

*NOTE 1 BS 10008-1 specifies the contents of information storage and transfer policy statements, which cover the scope of the policy, requirements for procedures and technology and the responsibilities of the management of the systems. BS 10008-1 also specifies the requirement for the top management team to set a clear policy direction and demonstrate support for, and commitment to, the management of the ESI through the issue and maintenance of these policies.*

The policy statements should be approved by the top management of the organization and reviewed for relevance and content at regular intervals. The frequency of review should be appropriate to the application.

*NOTE 2 This period is typically the same as the normal procedural audit cycle within the organization, for example, annual or in the event of major changes to the system.*

There is frequently more than one type of electronic identity management system in use within an organization. The identity requirements for each document type should be reviewed based on timeliness and service levels.

*NOTE 3 Cost might also be a consideration.*

In order to align electronic identity requirements with specific electronic documents, a document type designation should be allocated.

*NOTE 4 These types can be described by application (e.g. financial reports or stock lists) or by ESI content (e.g. an invoice or an order).*

The policy statements should set out guidelines for the appropriate application of an electronic identity for each document type. These statements should include the organizational requirements for identity, authority and copyright protection.

*NOTE 5 The underlying issue with these items is the requirement to understand the significance of an electronic identity attached to a document. If it is always someone within the same organization, it is significantly less complex than between organizations because the organization can set its own rules. For all inter-organizational documents controlled with electronic signatures or copyright protection, it is imperative that the recipient organization is capable of understanding the significance of what is communicated to it, recognizing, implementing and utilizing the relevant controls.*

#### **EXAMPLE**

For some electronic documents, it is important that the identity of the signatory is reliable and can be trusted. For other electronic documents, the actual identity of the author might not be important.

For example, an electronic order for goods of high value might need to be signed by an authorized member of staff. The receiving organization would have a list of approved signatories. The order would need to have a verifiable signature attached.

An order for a train ticket over the internet does not, however, need to be signed. The railway company is happy to receive the value of the ticket by the entry of validated credit card details. The identity of the traveller is not important to the transaction.

BS 10008-1 also specifies the contents of an information security policy within which the information storage policy operates. The information security policy statement should document the level and rigour of protection required, detailing the requirements for each document type.

Where there is a requirement, the policy statements should describe the degree of security required, for example, some documents are not as significant as others and proof of the identity of the signatories is of less importance – for instance, an internal memo as opposed to a contractual commitment.

Approved policy statements should be retained in compliance with the retention schedule (see [5.2.2.3.3](#)).

## **5.2.2 Information storage policy statement**

### **5.2.2.1 Structure**

*NOTE 1 This subclause describes documentation that states the information storage policy of the organization.*

Availability of this documentation should, when combined with appropriate proof of compliance, demonstrate (e.g. to a court of law) that responsible information storage is part of the normal business practice of the organization.

An information storage policy statement should be produced, documenting the policy on information storage. Policy objectives should be clearly stated, such that they can be easily interpreted and implemented.

The information storage policy statement should be approved by the top management of the organization, and should be reviewed for relevance and content at regular intervals. The frequency for review should be appropriate to the application.

*NOTE 2 This period is typically the same as the normal procedural audit cycle within the organization (e.g. annual or in the event of major changes to the system).*

The information storage policy statement should include the policy of the organization (for each document type) on:

- a) applicable protection techniques that may be used;
- b) responsibilities for the control and management of these techniques; and
- c) the control and management of keys and certificates (if used).

Where third parties are involved, the responsibilities and liabilities of those third parties should be clearly identified.

The information storage policy statement should also include the policy of the organization on:

- 1) the verification of the validity of certificates and signatures;
- 2) reacting to challenges to certificates and signatures;
- 3) where appropriate, the selection criteria for TTPs;
- 4) arbitration routes as an independent mechanism for enabling the resolution of disputed challenges; and
- 5) retention periods (and other information) for documents created during the verification process, including audit trail data.

*NOTE 3 [Annex C](#) includes an example information storage policy statement. It contains some “typical” statements that might be appropriate in many policy statements.*

The information storage policy statement should contain, as a minimum, those included below. Other sections may be added where appropriate.

- Scope (see [5.2.2.2](#))
- ESI classification (see [5.2.5](#))
- Standards related to information management (see [5.2.2.3](#))
- Compression (see [5.2.2.4](#))
- Electronic file formats (see [5.2.2.5](#))
- Database management systems and schemas (see [5.2.2.6](#))
- Roles and responsibilities (see [5.3](#))
- Applicable legislation (see [5.4](#))
- Legal and regulatory consultations (see [5.4](#) and [Annex D](#))
- Storage technology (see [8.13.1](#))
- Encryption (see [8.14.2.7](#))
- Identity (see [8.17](#))
- Retention schedule and disposal procedures (see [8.18](#))
- Auditing (see [9.2](#))

#### 5.2.2.2 Scope

The policy statements described in [5.2.2.1](#) might not cover all the different types of ESI that the organization uses. The ESI to be included in its scope should be identified and grouped into types,

with the policy for all ESI within a type being consistent. Where a retention schedule and disposal procedures (see [5.2.2.3.3](#)) exist, it might be appropriate to use the same ESI type groups.

Where formal records management procedures are implemented, ESI types will generally be used in classification schemes (file plans) and/or taxonomies. Where this is the case, the same file grouping and naming conventions should be used.

ESI types can be specified by reference to application (e.g. “financial projections”, “invoices” or “customer address list”) or by reference to generic group (e.g. “accounting data”, “customer documents” or “manufacturing documents”).

The policy statements should include, as one or more ESI types, all documents produced in conformance to BS 10008-1, as well as system and application audit trails (see [7.5.4](#)).

All ESI types should be included in the policy statements.

An alternative to this approach of including only identified ESI types in the policy scope can be adopted, since there is a risk that the organization might need to produce absolutely any of its ESI assets in the event of a dispute. The organization should consider whether it needs to have any ESI that is totally unmanaged, even the ESI that is regarded as of very low value to the organization.

In this case, it is worth considering whether the policy scope should include a “default” ESI type (with associated policy and policy implementation and compliance requirements) as well as the explicitly identified ESI types. ESI outside the scope of the explicitly identified types should be managed according to the default.

### 5.2.2.3 Standards related to information management

*NOTE This is not an exhaustive list of standards related to information management.*

#### 5.2.2.3.1 General

Frequently, business benefits can be achieved by complying with relevant national or international standards, codes of practice or other guides. The policy statements should state whether all or specific parts of any such publication(s) are to be complied with.

*NOTE The [BS EN ISO/IEC 27000](#) series of international standards are the UK reference documents for information security management.*

#### 5.2.2.3.2 Quality management

Where the organization operates a quality management system (such as one in accordance with BS EN ISO 9001), whose scope includes part or all of the information management system within the scope of compliance, then all documentation that BS 10008 requires should be included in the quality management system.

#### 5.2.2.3.3 Retention schedule and disposal procedures

A retention schedule should be established for each ESI type included in the policy statements and agreed with all relevant departments and personnel within the organization. The retention schedule should be reviewed at regular intervals.

*NOTE 1 Where appropriate, legal advice might be required to ensure that minimum legal and/or regulatory retention periods, as well as business requirements, are complied with.*

*NOTE 2 For further information and guidance on retention schedules, see:*

- the National Archives<sup>3)</sup>; and
- the Information and Records Management Society<sup>4)</sup>.

<sup>3)</sup> [www.nationalarchives.gov.uk/information-management/manage-information/](http://www.nationalarchives.gov.uk/information-management/manage-information/)

<sup>4)</sup> [www.irms.org.uk](http://www.irms.org.uk)

All documentation that BS 10008-1 and this British Standard require to be kept should be covered by the retention schedule.

There should also be a process for the controlled destruction (or other process such as the preservation as historical records) of ESI at the end of its retention period, i.e. a disposal schedule. In many instances, the disposal process involves the physical disposal of the ESI (including all copies). In other cases, ESI might be passed to archives (to allow it to be used for research and/or statistical purposes), in which case, policies should detail which documents (and maybe which information in these documents) are to be archived.

The retention schedule and disposal procedures should be included in, or referenced by, the policy statements, covering all ESI types included in the policy statements.

#### 5.2.2.4 Compression

*NOTE Some ESI needs to be compressed before being stored and/or transferred. This might be due to:*

- a) a large file size (a smaller, compressed file will require less transmission time);*
- b) a large number of individual files (these can be compressed into a single file); or*
- c) the application of a compression key to improve electronic document security.*

The policy statements should give guidance on when compression is to be used, and how to formulate compression keys.

#### 5.2.2.5 Electronic file formats

In order to facilitate effective storage, the organization should have policies regarding the use of specific types of medium for different information storage requirements (e.g. access requirements, retention periods and security requirements). These policies should be used to decide the medium to be used for the storage of each ESI type. These policies should be included in the policy statements. See [8.13.1](#) on storage technology.

The policy statements should contain details of the approved electronic file formats that may be used for each ESI type. Where the electronic file might be subjected to compression techniques (see [8.13.5](#)), their use should be documented.

#### 5.2.2.6 Database management systems and schemas

The policy statements should contain details of the approved database management systems (DBMS) and database schemas. Changes to approved DBMS and database schemas should be under an approved version control system (see [8.12](#)).

In the event of the DBMS and schema for a particular application or service being unavailable or unpublished proprietary intellectual property of a third party, the organization should assess the implications of the unavailability of this information and, if deemed acceptable, document this within the policy statements.

### 5.2.3 ESI transfer policy statement

#### 5.2.3.1 General

There are many forms of technologies and procedures that can be used for ESI transfers. The ESI transfer policy statement should give guidelines on the type of transfer technology to use in particular circumstances, on the content and layout of unstructured transfers and on the identification of the appropriate systems to be used for all corporate ESI transfers.

In particular, the use of structured and unstructured forms of ESI transfers should be included. Where unstructured ESI transfers are involved, corporate guidelines on message structures should be included within the ESI transfer policy statement, or referenced by it.

The ESI transfer policy statement should provide guidelines on the requirement for appropriate procedures to be followed when ESI transfers are being undertaken.

*NOTE* Details of these procedures can be found in [Clause 8](#). These procedures might need to link to the information security policy of the organization as detailed in [5.2.4](#).

#### 5.2.3.2 Delivery/receipt

The critical procedural issues are related to the delivery of and the receipt of ESI transfers, thus, the ESI transfer policy statement should give guidelines on how these procedures are to be developed, and to what standards, including where ESI transfers are sent and/or received. These procedures should include:

- a) the avoidance of messages with illegal content;
- b) the avoidance of copyright issues;
- c) protection against malicious software;
- d) appropriate security procedures;
- e) the application of the organization's retention and disposal policies; and
- f) the avoidance of spam and similar messages (incoming and outgoing).

#### 5.2.4 Information security policy

##### 5.2.4.1 General

*NOTE 1* It is essential that an organization is aware of the value of the information that is managed within the organization, or with its trading partners. This awareness includes an understanding of "duty of care" principles.

To fulfil its duty of care obligations, the organization should:

- a) be aware of and be able to demonstrate compliance with legislation and regulatory bodies pertinent to its industry;
- b) be aware of and be able to demonstrate compliance with legislation and regulatory bodies pertinent to its country (or other relevant geographical area) of origin, routing and/or receipt of electronic identity document attributes;
- c) establish a chain of accountability and assign responsibility for all relevant activities; and
- d) keep abreast of developments by keeping in contact with the appropriate bodies and organizations.

The implications of an insecure electronic information management system can be far reaching, and potentially damaging to an organization. In order to ensure the integrity of ESI, it should be managed under the controls specified in BS 10008-1.

*NOTE 2* If, however, ESI managed in compliance with BS 10008-1 is transferred by a system not conforming to the BS 10008-1, its evidential weight might be reduced.

Suitable guidelines, which specify system security requirements, might already exist in organizational policies or working practices. There might also be sector-specific guidance (e.g. financial or pharmaceutical), national or international standards, or legal requirements. Where these do not exist, suitable guidelines should be developed, approved and implemented.

##### 5.2.4.2 Information security policy

All electronic information management systems are vulnerable to compromise or change, whether accidental or malicious. To protect these systems, appropriate security measures should be

implemented to reduce the risk of such a compromise or change and thus a successful challenge to their effectiveness.

Security measures should be implemented which ensure that the application of electronic identity is controlled, reliable and auditable.

Similarly, security measures should be implemented to protect the ESI that is being secured using keys and/or certificates.

*NOTE 1 Such security measures are important, both for the organization and for a TTP.*

The organization should adopt an information security policy in relation to electronic information management systems. The use of electronic identity and authentication techniques, where appropriate, should be incorporated within the scope of the information security policy.

The organization should confirm that any TTPs that it uses have adopted their own appropriate information security policies.

Where document verification keys, certificates and other information are archived by a TTP, the organization should ensure that they are stored in compliance with that TTP's information security policy.

*NOTE 2 Compliance with the recommendations of [BS EN ISO/IEC 27002](#) is widely recommended; certification against [BS EN ISO/IEC 27001](#) is a way of demonstrating to other organizations that the above requirements on information security policy are being met.*

*Such independent accreditation is commonly regarded by TTPs as a means of proving their credentials to their customers. The tScheme publication, Guidance for Assessments, references compliance with information security management and formal accreditation against [BS EN ISO/IEC 27001](#). This certification is not mandated; it is a business decision of the TTP. The tScheme Guidance for Assessments (tSi0250) can be found in the tScheme Library: <https://www.tscheme.org/directory/library>.*

The information security policy should contain as a minimum:

- a) a scope statement;
- b) management objectives regarding the security of ESI;
- c) the security requirements for different ESI classification categories;
- d) the allocation of information security responsibilities;
- e) segregation of roles;
- f) access rights and the sharing of ESI;
- g) procedures for dealing with security breaches;
- h) a policy regarding compliance with appropriate standards (see [5.2.4.3](#)); and
- i) an approval and review process.

Different types of ESI might require different security techniques. These should be documented in the information security policy statement.

The organization should ensure that its own information security requirements are met by any chosen TTP. The TTP might not wish to publicize actual security procedures, but it should be ensured that it is able to demonstrate to the organization that it is compliant with the requirements of the organization.

The information security policy statement should be approved by the top management. The organization should then agree and document appropriate levels of security for managing its ESI, in compliance with its stated information security policy.

#### 5.2.4.3 Information security management standards

*NOTE 1* Information security standards provide auditable systems that enable organizations to demonstrate a duty of care in relation to managed ESI. [BS EN ISO/IEC 27002](#) gives recommendations on information security management. Proof of compliance with the recommendations of [BS EN ISO/IEC 27002](#) when implemented within the boundaries covered by this British Standard might provide helpful, supporting evidence in court or other dispute. It can indicate that the organization has exercised its duty of care, and it can assist the adjudicator in assessing the authenticity and integrity of the ESI.

*BS EN ISO/IEC 27001* is an auditable specification for use in the certification of an information security management system.

Compliance with the recommendations of [BS EN ISO/IEC 27002](#) or certification against [BS EN ISO/IEC 27001](#) should not be regarded as an alternative to compliance with the recommendations of this British Standard.

*NOTE 2* Compliance with the requirements of [BS EN ISO/IEC 27001](#) is predicated upon the proven quality management approach of demonstrably meeting a stated requirement, as defined by the organization in question. As such, this enables [BS EN ISO/IEC 27001](#) to be applied to organizations as varied as a government department, a high street bank and a consultancy employing one or two people. Clearly, the risks associated with these businesses are different and the information security measures adopted are, therefore, also different.

This British Standard works on a different premise to [BS EN ISO/IEC 27001](#). When ESI is used as evidence in the event of a dispute, the maximum weight of evidence is not affected by the size or shape of the organization and its own view of security risks. It frequently depends upon the opinion of an independent arbiter. That view might well be affected by the opposing party in the dispute attempting to discredit the evidential value. Therefore, this British Standard is based upon more prescriptive, less interpretative principles, and compliance with its recommendations is significantly more absolute than compliance with the requirements of [BS EN ISO/IEC 27001](#).

#### 5.2.4.4 CIA principle

*NOTE* [BS EN ISO/IEC 27001](#) includes details of an information security model, classifying information security into three areas (the "CIA" principle):

- a) confidentiality;
- b) integrity; and
- c) availability.

The relevance of all three of these principles should be reviewed and suitable procedures and processes implemented.

#### 5.2.4.5 Confidentiality

*NOTE* Whilst confidentiality is not necessarily an evidential weight or legal admissibility issue, and because similar cryptographic techniques are often used, this British Standard also provides guidance for the provision of confidentiality issues by ensuring that the ESI cannot be seen by unauthorized individuals. Confidentiality of ESI is typically handled by applying cryptographic encoding to the ESI, so that it can be accessed only by someone having the appropriate decoding processes and keys.

Where appropriate, ESI being managed should be protected from unauthorized access. Ensuring confidentiality in electronic information management should be as appropriate to business needs.

#### 5.2.4.6 Integrity and authenticity

*NOTE 1* Integrity is about ensuring that the content of a data file is unchanged; authenticity is about ensuring that it is what it purports to be. Both integrity and authenticity are key to the achievement of strong evidential weight and legal admissibility, ensuring data accuracy and completeness.

Whilst integrity applies to ESI that is captured and controlled by the management system that is the subject of the British Standard, the issues of authenticity apply to the information prior to capture

and are, as a consequence, outside the scope of the management system. Therefore, the organization should establish and operate procedures that ensure the authenticity of ESI that is captured by or imported into organizational systems (see 8.2 and 8.3).

When considering security, the risk of integrity or authenticity being compromised should be assessed and compared with the cost of protection against such compromise.

*NOTE 2 Security measures may include the application of encryption technology to reduce the risk of changes to ESI.*

Procedures and processes should be implemented to ensure the integrity of ESI during transfer. Processes and procedures should be adopted in relation to the value to the organization of the ESI being transferred.

*NOTE 3 Some systems use file names linked to message authentication codes (MACs) or digital signatures for this purpose (see 8.19.4).*

Data recovery procedures, to be implemented in the case of failure of the electronic information management system, should be such that they maintain the integrity of the relevant data.

#### 5.2.4.7 Availability

*NOTE 1 Availability is about ensuring that the ESI is available when it is required by an authorized user. Loss of ESI could be interpreted as being just as significant as fraudulent modification. It might be necessary to demonstrate that specific ESI is still available for a legally stipulated time after transfer. In this area, topics such as regular backup and business continuity planning are critical.*

Procedures and processes should be implemented to ensure that the ESI is available as required.

*NOTE 2 This can be implemented by managing ESI in compliance with BS 10008-1.*

#### 5.2.4.8 Copyright protection

Where electronic copyright protection systems, such as digital rights management (DRM), are used, care should be exercised because the use of such systems might control accessibility, potentially rendering content access impossible when required for dispute resolution evidential purposes.

If the organization is using DRM or has ESI that is under the control of a DRM system, the organization should consider and document how to maintain access availability to the ESI for the retention period as specified in the retention schedule of the organization.

*NOTE DRM is the technological protection measures that allow owners of copyrighted digital content to control digital content after an ordinary contractless sale of the content and prevent breaches of copyright law because of the ease with which digital files can be copied and transmitted.*

*DRM systems take two approaches to securing content. The first is "containment" for access control, an approach where the content is encrypted in a shell so that it can only be accessed by authorized users. The second technique is "marking", the practice of placing a watermark, flag or XML tag (see BS ISO/IEC 21000-5) on content as a signal to a device that the media is copy-protected. These two approaches are not mutually exclusive and can be combined.*

#### 5.2.4.9 Information security management framework

##### 5.2.4.9.1 Introduction

Where an appropriate information security management framework does not already exist, one should be established. It should control the information security management system as implemented within the organization.

The framework should have as its objectives:

- a) approval and review of the information security policy;
- b) monitoring of threats to information security;

- c) monitoring and review of security breaches; and
- d) approval of major initiatives to enhance information security management.

#### 5.2.4.9.2 Management objectives

*NOTE 1 All information, irrespective of the storage technology, is vulnerable to loss or change, whether accidental or malicious.*

To protect ESI, security measures should be developed and implemented to reduce the risk of a successful challenge to its authenticity. These security measures should be aligned to any ESI classification categories (see [5.2.5](#)) that are used.

*NOTE 2 Traditionally, information security is considered a matter of confidentiality, to ensure that ESI is not available for viewing outside the requirements of the organization. However, whilst this is important (in some cases, vital) to the operation of the organization, it is not the most important security issue relevant to compliance requirements.*

When developing security measures, the risk of integrity being compromised should be compared with the cost of the implementation of such measures. Security measures should include backup and other copies of ESI, as their integrity is of importance in circumstances in which they have been used as replacements for “live” data, or for use as “legal” archives.

*NOTE 3 There is also the important issue of availability. In some cases it might be necessary to be able to demonstrate that all ESI on a specific topic is available for review at any time. In such instances, issues such as indexing accuracy and business continuity planning are important.*

*NOTE 4 Security is not singularly a concern with computer systems. Security and availability of the operating environment (including buildings, temperature controls, network links, physical media, etc.) and the auditable implementation of procedures by all staff are all key elements.*

A management statement should be produced, detailing the organization’s strategy for information security management, upon which the information security policy (see [5.2.4.2](#)) is based.

##### EXAMPLE

An example of a management statement in relation to information security management is as follows.

The management objectives of this information security policy are to:

- ensure that ESI is accurate, complete and available as required;
- demonstrate continuity of information management services; and
- minimize business damage by preventing or minimizing the impact of information security incidents.

#### 5.2.4.10 Security breach management

*NOTE From time to time, security breaches, whether actual or suspected, arise with information management systems, and these breaches require emergency procedures to be implemented in order to recover from them. Such procedures might involve the temporary use of additional or third-party resources.*

In order to ensure that the integrity of ESI is not compromised during recovery operations, an agreed and approved information security incident management plan should be implemented.

Security breaches should be managed in a controlled manner, using procedures that ensure (or highlight any actual or potential issues concerning) the maintenance of the integrity of ESI, during and after an incident.

In some instances, the security breach might not appear to have affected the ESI. However, checks should be made to demonstrate that the integrity of the ESI has not been compromised.

In order to ensure that recovery from a security breach that resulted in major equipment, environmental or personnel failure has been successful, procedures should be developed, tested,

implemented and maintained. Such procedures should ensure that the integrity of ESI is not compromised during their implementation.

Where complete recovery from the results of a security breach cannot be assured, details of all actual or potential compromise to the ESI should be documented.

### 5.2.5 Information classification

*NOTE 1 In some applications, it is appropriate to implement an ESI classification system. Typically ESI classification systems are used to indicate the accessibility of particular documents to workers and other individuals. In government and other public bodies, this is often indicated by the use of security "labels" such as "top secret", "classified" or "publicly available". In the private sector, security classification schemes might be aligned to departmental requirements (such as accounts, credit control or customer services).*

If an ESI classification system is implemented, it should be simple to understand, and thus easy to implement. It should be based on need, priority and degree of protection needed. Excessive classification levels should be avoided.

*NOTE 2 One such scheme used within government is the Government Security Classifications. For more information, see [www.gov.uk/government/publications/government-security-classifications](http://www.gov.uk/government/publications/government-security-classifications).*

*NOTE 3 The organization can consider using an Information Classification, Marking and Handling (ICMH) scheme that conforms to the requirements of BS 10010 and can simplify compliance with BS 10008-1. For more information on classification, see BS 10010.*

As some ESI might be considered to be more significant and thus more likely to be used as evidence in the resolution of disputes, ESI users should be able to distinguish such significant ESI from other, less significant ESI, and consequently handle all ESI, whatever significance is attached to it, with the appropriate controls.

Where an ESI classification system is implemented, the information storage policy statement should include the details of classification with each ESI type and should align security measures to that classification system.

## 5.3 Roles and responsibilities of workers

### 5.3.1 General

The organization should identify, define and document the roles and responsibilities of all workers, to ensure compliance with BS 10008-1.

### 5.3.2 Top management

It is the responsibility of top management to identify and appoint appropriate resource to ensure compliance with BS 10008-1. This should include:

- a) accountability to the organization for the management of ESI;
- b) stewardship of ESI (see 5.3.3); and
- c) day-to-day management of ESI (see 5.3.4).

*NOTE These roles and responsibilities may be undertaken by a single individual or by multiple individuals, dependent upon the size of the organization and the complexity of the ESI.*

### 5.3.3 Information stewards

Information stewards should operate in a business-focussed manner, and should be aware of the business systems that manage ESI and the risks involved in the implemented technology and procedures.

### 5.3.4 Responsibility for managing the system

#### 5.3.4.1 General

The responsibility for system management should be either an organization-wide role or should be organized at a departmental/functional level. Where a split role is implemented, there should be a mechanism for coordination across the organization, to ensure that common policies and practices are established.

#### 5.3.4.2 Roles and responsibilities of workers

Roles and responsibilities for information management and information security management should be defined in the relevant policy statements.

*NOTE 1 These roles and responsibilities may extend outside the organization, where third parties have access to systems.*

*NOTE 2 The responsibilities in relation to information management may be indicated with reference to a job function (e.g. the IT manager).*

Responsibilities in relation to information management should be assigned for:

- a) policy statement content;
- b) policy statement approval (typically a senior board member);
- c) policy statement periodic review;
- d) information content of each ESI type defined;
- e) the information management system; and
- f) ensuring continued compliance.

*NOTE 3 The responsibilities in relation to information security management may also be indicated with reference to a job function (e.g. the information security manager).*

Responsibilities in relation to information security management should be assigned for:

- 1) security policy content;
- 2) security policy approval (typically a senior board member);
- 3) security policy periodic review;
- 4) security classification for each ESI type defined;
- 5) the information security management system; and
- 6) ensuring continued compliance.

#### 5.3.4.3 Segregation of roles

*NOTE 1 The segregation of roles is a fundamental aspect of duty of care. It provides a check on errors and on the deliberate falsification of records (in this respect, segregation of roles is particularly important in management systems where there is risk of fraud or other malicious action).*

There are several aspects of information management where segregation of roles should be considered and implemented where appropriate:

- a) input reconciliation;
- b) quality control;
- c) data entry;
- d) ESI disposal; and
- e) ESI security.

It should be ensured that the physical and managerial segregation that exists around a system is mirrored by the logical access controls within it.

In some instances, segregation of two roles might not be feasible, due, for example, to the lack of availability of alternate workers. A justification in this case should be documented. For example, where the scanner operator checks the quality of images during the scanning procedures, a second quality control procedure should be undertaken by personnel other than those responsible for the scanning.

*NOTE 2 This second quality check may involve systematic sampling.*

Any procedure that is self-checking should be identified, including where there is a potential risk to the integrity of procedures.

Procedures should be modified where necessary to ensure system reliability.

#### 5.3.5 All ESI users

Any workers that have access to ESI should be aware of their roles and responsibilities when handling the ESI.

*NOTE This includes ensuring that ESI is captured in the correct location within the information storage system, and that the correct ESI is transferred to the correct recipient.*

### 5.4 Legal and regulatory environment

*NOTE 1 It is important to be aware of the various legal and regulatory requirements that the organization needs to comply with, which might include multiple jurisdictions. Some (or maybe all) of these require the keeping of information. Some legal advisers or regulators might be unfamiliar with electronic information management systems, and so will need to seek consultation before a “mainly electronic” process is implemented.*

*Typical bodies that might need to be consulted are:*

- a) regulatory bodies;
- b) government bodies;
- c) external audit bodies; and
- d) legal advisers.

*These consultations might need to include the following topics:*

- 1) legal issues (civil law and/or company law);
- 2) government regulations; and
- 3) special regulations (applicable to particular sectors).

*These consultations might be appropriate at different levels, which can include:*

- national and international law;
- industry sector regulation;
- community by-laws;

- *organizational policies;*
- *departmental procedures; and*
- *individuals' rights.*

Relevant consultations should be made to ensure that the organization is aware of, and thus can comply with, all appropriate legal and/or regulatory requirements.

The results of all consultations, including actions agreed, planned or implemented, should be referenced or included in the policy statements.

*NOTE 2 For further information on legal issues, see [Annex D](#).*

---

## 6 Planning

### *COMMENTARY ON CLAUSE 6*

*This clause of this British Standard relates to BS 10008-1:2020, Clause 6.*

### 6.1 Actions to address risks and opportunities

#### 6.1.1 General

When planning for the management of the authenticity and integrity of ESI, the organization should consider the issues referred to in [4.2](#) and the requirements referred to in [4.3](#) and determine the risks and opportunities that need to be addressed to:

- a) ensure the information management system can achieve its intended outcome(s);
- b) prevent, or reduce, undesired effects; and
- c) achieve continual improvement.

The organization should also plan:

- 1) actions to address these risks and opportunities; and
- 2) how to:
  - i) integrate and implement the actions into its information management system processes; and
  - ii) evaluate the effectiveness of these actions.

#### 6.1.2 Risk assessment

*NOTE 1 Information management procedures are often developed in an unstructured way, by reacting to user requirements, security incidents and/or to available computer software tools. This approach on its own can easily leave gaps in information management, which are only filled at some later date, typically after a security breach. A more structured approach is to review the ESI assets of the organization and assign risk factors (based on asset value, potential threats, system vulnerability and likelihood of attack), on the basis of which appropriate, cost-effective information management procedures can be identified.*

An essential part of information management is the implementation of an appropriate information security policy, which should be produced and approved, based on a risk assessment, and against which security measures can be developed and implemented.

*NOTE 2 A review of this type generally requires security expertise and a range of appropriate technical skills.*

The organization should undertake an information security risk assessment along these lines, and document the results obtained. Of particular importance are the security measures implemented to control the information storage media, both the “live” media and the “backup” media. The risk

analysis should include vulnerability risk factors consistent with the type of medium being used (e.g. WORM or rewritable).

On the basis of the results of the risk assessment, existing security measures should be reviewed for effectiveness. Factors such as the balance between the cost of implementation and the security achieved should be taken into consideration during the review process. Where the review indicates that changes to security measures are appropriate, an action plan should be drawn up with new or amended security measures prioritized for implementation.

*NOTE 3 The risk assessment will lead to the acquisition of information and the creation of risk reports. These reports, backed up by the information used to develop the conclusions and recommendations in the reports, might provide useful evidence in relation to information management decisions made by the business.*

Information related to risk assessments should be retained in line with the retention schedule.

*NOTE 4 BS ISO 31000 provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. It can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.*

### 6.1.3 Risk treatment

The results of the risk assessment should be used to guide and determine the appropriate management action and priorities for managing information risk and implementing controls selected to protect against those risks.

*NOTE 1 BS ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review. It describes the input to a risk treatment process as a list of identified risks, prioritized according to the risk evaluation criteria of the organization. Risk treatment includes the identification and implementation of controls to reduce, retain, avoid or share the identified risks.*

Risk treatment should be implemented by one or more of the following non-exclusive processes:

- a) risk modification;
- b) risk retention;
- c) risk avoidance; and/or
- d) risk sharing.

*NOTE 2 Risk modification involves the addition, removal or modification of existing controls such that the residual risks can be re-evaluated.*

*NOTE 3 Risk retention is the process of retaining an identified risk without further action. This is acceptable where the identified risk is within the agreed risk criteria.*

*NOTE 4 Risk avoidance involves the removal of processes related to the risk, such that the risk is no longer present. This may be used where the cost of other forms of risk treatment are too costly to implement.*

*NOTE 5 Risk sharing involves the sharing of the identified risks with other parties, such as by insurance or by subcontracting particular processes.*

## 6.2 Objectives and achievements

The organization should establish information management objectives at relevant functions and levels.

The information management objectives should:

- a) be consistent with the information storage policy;
- b) be measurable (if practicable);
- c) take into account applicable information management requirements and results from risk assessment and risk treatment;
- d) be communicated; and
- e) be updated as appropriate.

The organization should retain documented information on the information management objectives.

When planning how to achieve its information management objectives, the organization should determine:

- 1) what will be done;
- 2) what resources will be required;
- 3) who will be responsible;
- 4) when it will be completed; and
- 5) how the results will be evaluated.

---

## 7 Support

### COMMENTARY ON CLAUSE 7

*This clause of this British Standard relates to BS 10008-1:2020, Clause 7.*

### 7.1 Resources

The organization should determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information management system.

### 7.2 Competence

The organization should:

- a) determine the necessary competence of person(s) doing work under its control that affects its information management performance;
- b) ensure that these persons are competent on the basis of appropriate education, training or experience;
- c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- d) retain appropriate documented information as evidence of competence.

*NOTE* Applicable actions might include, for example, the provision of training to, the mentoring of, or the reassignment of current workers; or the hiring or contracting of competent persons.

### 7.3 Awareness

Workers doing work under the control of the organization should be made aware of:

- a) the information storage policy;
- b) their contribution to the effectiveness of the information management system, including the benefits of improved information management performance; and
- c) the implications of not conforming to the information management system requirements.

## 7.4 Reporting and communication

When developing policies and procedures, it should be ensured that:

- a) information related to the policies and procedures is made available to those that are or might be affected by them;
- b) there is a mechanism for feedback from the implementers of the policies and procedures;
- c) there is a mechanism for reviewing risks related to the policies and procedures;
- d) details of any challenges to the authenticity and/or integrity of ESI is fed back to those responsible for compliance with BS 10008-1 and this British Standard; and
- e) the methods used for these communications are regularly assessed for effectiveness and updated where necessary.

This documentation should be retained in compliance with the retention schedule.

## 7.5 Documented information

### 7.5.1 General

Documented information related to the process of managing ESI should be created, captured and retained for as long as necessary. [Subclause 7.5.2](#) details procedural documentation that should be created and retained.

*NOTE This subclause also includes information related to the management of this ESI, including the requirement for version control and appropriate retention periods.*

### 7.5.2 Procedural documentation

#### 7.5.2.1 General

Compliance with BS 10008-1 and this British Standard requires the availability and use of specified documentation. This documentation consists of the:

- a) information storage policy statement (see [5.2.2](#));
- b) information retention schedule (see [5.2.2.3.3](#));
- c) information security policy statement (see [5.2.4](#));
- d) procedures documentation (see [7.5.2.2](#));
- e) system description documentation (see [7.5.3](#)).
- f) ESI transfer policy statement (see [5.2.3](#))

The availability of these documents, and demonstrable adherence to the procedures they describe, should, if effectively constructed, provide the audit trail that can be used to demonstrate the authenticity of ESI, and so enhance its evidential weight.

Each of the documents mentioned in a) to e) may be maintained as a separate document, or these documents may be combined. Whether separate or combined, the documentation should exist, be maintained and be readily accessible to those authorized within the organization to access it and to any authorized third party who might require access.

All documentation should be maintained in line with existing working practices, and should be maintained under a version control system (see [8.12](#)).

*NOTE 1 Additional documentation might be required to support the daily operation of the system, for example:*

- *the system maintenance log (see [8.17.14](#));*
- *an audit trail (see [7.5.4](#));*
- *compliance statements (see [9.3.4](#)).*

The content of the documentation in a) to f) can easily become unreliable where there are no procedures in place to ensure that they keep pace with both organizational and system changes. Unreliable documentation can adversely affect legal arguments relating to the correct operation of an information management system. It should be ensured, therefore, that the definitive versions of system documents are brought under configuration management control, and are firmly linked to the change management procedures of the organization.

Where compliance with BS 10008-1 and this British Standard is claimed over a period of time during which different editions of the documentation in a) to f) were appropriate, then all editions of this documentation should be kept in compliance with the policies.

*NOTE 2 This is to ensure that, where information regarding the system at a point in the past is required, it can be obtained from this document store.*

*NOTE 3 Documentation is essential evidence for the policies, procedures and technology used. It is part of the system audit trail.*

## **7.5.2.2 Procedures documentation**

### **7.5.2.2.1 General**

The organization should maintain documentation (procedures documentation) for each information management system conforming to BS 10008-1 and this British Standard, describing all procedures related to the operation and use of the system, including input to, operation of and output from the system.

*NOTE 1 This documentation can include references to other controlled documentation as appropriate.*

*NOTE 2 For convenience, procedures documentation may be maintained as a number of different elements relating to different information management areas. Where the organization has multiple information management systems, the documentation may comprise a single procedures document or multiple procedures documents.*

Procedures documentation should be readily accessible to all appropriate users of the system.

### **7.5.2.2.2 Content**

Procedures documentation should include the topics listed below.

- a) ESI capture
- b) Self-modifying files
- c) Compound documents
- d) ESI in structured databases
- e) Big data considerations
- f) Blockchain/distributed ledger technology (DLT)
- g) Version control
- h) Storage systems
- i) Information retention
- j) Information redaction
- k) Information disposal

- l) ESI transfer
- m) Identity authentication
- n) Transfer
- o) Receipt of a transfer
- p) Indexing
- q) Output
- r) Identity
- s) Information security procedures
- t) System maintenance
- u) External service provision
- v) Information management testing

### 7.5.3 System description

#### 7.5.3.1 General

A description of hardware, software and network elements that comprise the system and how they interact, including details of system configuration, should be recorded and made available (the system description documentation). It should be structured so that details of the system at any time during the period of its use can be readily accessed.

*NOTE 1 This can be achieved by creating a new version of the documentation every time there is a change, or by including a "change control" section in the documentation. What is important is that there is a clear description of the system as it was at a particular time in the past.*

*NOTE 2 For systems already in operation, information stored on the system prior to the introduction of BS 10008-1 and this British Standard cannot be considered as meeting its provisions unless the controls and procedures described in BS 10008-1 and this British Standard have been in place from the time of storing that information.*

Where the information storage policy requires compliance with particular national and/or international standards, the system description documentation should include a section demonstrating compliance with those standards.

*NOTE 3 This enables system auditors to check the performance and reliability of the system against these standards.*

#### 7.5.3.2 Content

The system description documentation should include the topics listed below.

- a) Storage systems
- b) Environmental considerations
- c) Media migration
- d) Format conversion
- e) Compression techniques
- f) Workflow, business process management (BPM) or robotic process automation (RPA) systems
- g) Access rights
- h) Encryption
- i) Digital signatures

- j) Other authentication techniques
- k) Audit trails
- l) Date and time stamps
- m) Transfer initiation
- n) Integrity checks
- o) Sender and recipient authentication
- p) Identity authentication
- q) Identification of information
- r) Transfer systems
- s) Interim or temporary information storage
- t) Confirmation of receipt

### 7.5.3.3 Maintenance of documentation

Compliance with BS 10008-1 and this British Standard requires the availability and use of specified documentation. Maintenance of this documentation should be in accordance with the requirements of BS 10008-1 and the recommendations of this British Standard, including the keeping of records of this maintenance. This documentation should be subject to records management disciplines that are at least as good as those applied to the other records fundamental to the functioning of the organization.

*NOTE 1 Organizations might have a framework for managing their records in accordance with BS ISO 15489-1.*

There should be documented procedures for ensuring that documentation is up to date.

It should be ensured that the version appropriate at a particular point in time in the past can be identified and accessed.

*NOTE 2 Maintenance is required because, over time, requirements evolve and technologies and legislation change. In some cases, it will suffice for maintenance efforts to be driven by recognition of changes, on an ad hoc basis. Additionally, typically for more important documents, a routine regular review is appropriate. In most cases, it is desirable for changes to be documented in a way that allows a stakeholder to track the changes between versions. This can be implemented by recording a simple change history for each part of the documentation.*

*NOTE 3 Documentation may be stored electronically in the information management system, subject to the same controls as included in BS 10008-1 and this British Standard, or in analogue form (e.g. paper) in secure locations.*

### 7.5.3.4 Updating and reviews

It should be ensured that the procedures implemented at any time during the storage life of any specific piece of ESI can be determined. The procedures documentation (see [7.5.2.2](#)) should be kept up to date, and all previous versions should be kept in compliance with the information storage policy (see [5.2.2](#)).

All changes to operational procedures should be managed by a change control procedure, and should include updating the procedures documentation.

Superseded versions of the procedures documentation should be kept in compliance with the retention schedule, together with the dates during which they were in operation.

Procedures documentation should be regularly reviewed to ensure that it is up to date.

All changes should be reviewed to ensure that compliance with BS 10008-1 and this British Standard is not compromised.

## 7.5.4 Audit trails

### 7.5.4.1 General

*NOTE* When preparing ESI for use as evidence, it is often necessary to provide further supporting information. This information might include details such as date of storage of the ESI, details of movement of the ESI from medium to medium, and evidence of the controlled operation of the system. These details are known as “audit trail” information. This audit trail information is needed to enable the working of the system to be demonstrated, as well as the progress of ESI through the system, from receipt to final deletion.

#### 7.5.4.1.1 Purpose and generation

*NOTE 1* The audit trail as defined for BS 10008-1 and this British Standard consists of the aggregate of the information necessary to provide a historical record of all significant events associated with the ESI and the information management system. As such, it covers the answers to all the classic questions concerning the provenance of any piece of information stored within the information management system:

- Who?
- What?
- Where?
- When?
- Why?
- How?

These audit trail details can be split into two categories:

- a) system (including the hardware platform(s), applications and operating software, configuration, and processes and procedures); and
- b) stored ESI.

In most organizations, the audit trail consists of a collection of system- and operator-generated logs.

*NOTE 2* For further advice on audit trails and on building information management systems that are “fit for audit”, see PD 0018.

Audit trail data should, as far as practicable, be generated automatically by the system, and the system description documentation (see 7.5.3) should describe the processes. In this case, the data should be created and stored immediately following the event that is being audited. Audit trail data should include entries for all system and data changes.

Where audit trail data are not generated automatically by the system, procedures for their manual (or other) generation should be implemented. In this case, the data should be created as soon as possible after the event that is being documented. For example, when an operator completes a task, the time should be recorded as soon as possible after the task was completed. If the record is of when preparation of a particular batch of documents was started, the time should be recorded just before the preparation of that batch commences.

It should not be possible to make any changes to the system or the ESI within the system without creation of an audit trail entry.

It should not be possible to amend audit trail data. Deletion should be possible only in accordance with the retention and disposal policy of the organization.

#### 7.5.4.1.2 Content

##### 7.5.4.1.2.1 General

Audit trails should be comprehensive and properly looked after, as without them the integrity and authenticity, and thus the evidential weight, of the information stored in the system could be called into question.

The audit trail content is critical, as it can be used to determine the relevance and importance of particular document types. Audit trails might also be needed to audit such activities as creation, access and deletion. Thus, the audit trail should include a record of all relevant occurrences.

*NOTE 1 If any significant occurrence is not audited, then the whole audit trail can be discredited and, as a direct result, all or any ESI held within the system might also be discredited.*

Technologies for electronic information storage should be chosen with audit trail requirements in mind.

*NOTE 2 This could result in technologies being rejected that might otherwise have appeared suitable for a particular application.*

When choosing electronic information storage systems, suitable audit trail functionality should be considered as a basic system requirement.

Audit trails should include details related to the following procedures:

- a) information creation (see [8.2](#)) or import (see [8.3](#));
- b) indexing and other metadata (see [8.15](#));
- c) version control (see [8.12](#)); and
- d) disposal of ESI (see [8.18](#)).

All audit trails should include details of who the individual was or what application/system component was responsible for the audited event.

##### 7.5.4.1.2.2 Information capture/importation

*NOTE 1 Audit trail data about the information capture process provides invaluable information to assist in the authentication of ESI. Details such as capture time, operator and capture device can prove vital when authenticity is challenged.*

Records should be kept in the audit trail of key information concerning ESI captured by or imported into the system.

*NOTE 2 Information that is typically stored in the audit trail includes:*

- a) document or file identification;
- b) device identifier;
- c) process date and time stamp;
- d) process duration (e.g. for video files);
- e) batch reference (for batch input);
- f) number of pages (for document scanning) or data records (data capture);
- g) quality control check approval;
- h) an identifier for each document or file that was indexed;
- i) worker and workstation identifier; and
- j) final write to storage.

*The choice of actual data to be stored in the audit trail depends upon the application and the system.*

Where individual files are captured or imported, audit trail data should be kept on a file-by-file basis.

*NOTE 3 This is particularly relevant where data files are imported into the system. In this case, the following audit trail information can be stored:*

- a) a unique file identifier;
- b) number of documents/pages/data records within the file;
- c) size of the file (e.g. kilobytes); and
- d) file format.

Where compound files are captured or imported, audit trail data should include the relationship between the parts.

#### 7.5.4.1.2.3 Batch processing

*NOTE Where batch processes are involved, it is common to use batch control documents to record and reconcile batch content and process completion. These form an integral part of the overall audit trail. It may be appropriate to audit at the batch level rather than the individual document level in some parts of the creation and storage processes.*

Where data are captured or imported on a batch basis, particularly in document scanning applications, the following audit trail information should be stored:

- a) unique batch identifier;
- b) operator identifier;
- c) type of material scanned (e.g. paper documents, roll microfilm and/or aperture cards);
- d) quantity of material in the batch (e.g. number of documents, number of pages (single/double-sided) or number of microfilm frames); and
- e) details of image processing performed during the scanning process, where this is different from any default image processing described in the system description documentation.

Audit trail data should be stored so that it is easy to confirm that:

- 1) all required activity has been performed for that batch;
- 2) details of any anomalies or discrepancies that have been encountered (e.g. number of pages written to storage not agreeing with number of pages scanned) have been recorded and dealt with;
- 3) quality control procedures have been completed; and
- 4) required exception processing has been completed.

When working in batches, audit trail data should include relevant information about batch reconciliation.

#### 7.5.4.1.2.4 Indexing

*NOTE 1 Indexing information is vital to the ESI retrieval process, and so its accuracy is key to establishing the authenticity of ESI. Audit trail information detailing the creation and modification of indexes can be used to demonstrate that indexing procedures have been correctly followed.*

*NOTE 2 It might be appropriate, depending upon the application, to keep "before" and "after" records of index entries that are amended or deleted.*

Where an index item relates to deleted ESI, this fact should be documented.

A record should be kept in the audit trail of the date and time of the creation, amendment and deletion of every index file.

Audit trail data should include an identifier for each document or data file that is indexed.

#### 7.5.4.1.2.5 Version control

Where a change is made to a data file, audit trail data should be created and stored, identifying the nature and details of the change.

*NOTE* Such changes could have been made by an individual, or automatically by the system.

Where appropriate, previous versions of data files should be referenced in the audit trail data, to identify the nature of the change.

#### 7.5.4.1.2.6 Disposal of ESI

Records should be kept in an audit trail of the disposal of ESI at the end of the relevant retention period.

*NOTE* This is particularly significant if it is necessary to demonstrate that ESI disposal was in accordance with the retention schedule and disposal procedures and was not undertaken to hide ESI that could have been incriminating evidence.

Where original documents are destroyed following a scanning process, records should be kept in an audit trail of the destruction of the original documents.

#### 7.5.4.1.2.7 Security of audit trails

*NOTE 1* If the authenticity of ESI is questioned, the integrity of the audit trail might be fundamental in establishing the authenticity, and thus the evidential weight, of the ESI. If the possibility exists that the audit trail data could be modified, this will reduce the evidential weight of any ESI to which these records apply.

The audit trail should be kept at the level of security appropriate to preventing any change to any data within it, and in accordance with the information security policy, as well as the retention and disposal policy, of the organization.

The audit trail should be subject to internal records management policies and procedures that are at least as good as other records fundamental to the functioning of the organization.

Secure backup copies of the audit trail should be kept, including automated and manual audit trail data.

*NOTE 2* Organizations might have a framework for managing their records in accordance with BS ISO 15489.

Where file recovery procedures have been implemented, sufficient audit trail data should be stored to demonstrate that the recovery did not affect the authenticity of ESI.

Wherever possible, audit trail data should be stored in an unmodifiable form. Where this is not possible, security measures should be used to ensure that it is not modified.

To minimize risk, audit trail data should be stored on WORM media. If a rewritable medium is used, then additional procedures should be implemented to reduce the risk of changes being made.

*NOTE 3* The use of magnetic tape makes it relatively difficult to modify data, as magnetic tape is normally a serially written medium.

If audit trail data has been modified, then any such modification should be audited.

Paper documents used for audit trail data should be frequently removed from the place of use and stored securely.

Users should assess such risk when using paper for audit trail records. Where paper documents are used, copies of them should be stored on the information management system.

*NOTE 4* The longer a document used for audit trail data (e.g. operator logs) is left in a relatively insecure place, for example, at a workstation, the higher the risk of tampering.

#### 7.5.4.1.2.8 Management

Audit trail information should be properly managed, as it might be of critical importance to the organization.

*NOTE 1 Any claims of compliance with organizational policies could be discredited if the audit trail is not treated correctly and cannot be interpreted unambiguously.*

*NOTE 2 Where audit trail data are stored manually by an operator, it might be impractical and unnecessary to create audit trail data on a per document basis. For example, when undertaking document preparation for scanning, it may be sufficient to document the date and, where appropriate, time at which preparation of a batch of documents started and ended. It may suffice to document simply when the operator started and ended work, provided it is possible to identify subsequently which operator prepared which documents.*

It should be ensured that the audit trail data are authentic, accessible, sufficiently comprehensive and understandable.

Audit trail data should include a date and (where appropriate) time stamp (see [7.5.4.2](#)).

#### 7.5.4.1.2.9 Storage and retention

*NOTE 1 The storage of audit trail data is a topic often not included in information storage policies. As the storage of audit trail data is frequently created automatically, and infrequently accessed, it is often forgotten, and thus not subject to adequate control.*

To ensure that all relevant audit trail data are stored, “audit trail data” should be included as a specific document type in the information storage policy. It should be stored for at least as long as the ESI to which it refers.

*NOTE 2 Some systems control the size of audit trail data files by the use of “looping”, which sets the maximum size for the data file, and when this size is reached, new data overwrite the oldest data in the file. Thus, old audit trail data are lost. This process might not be in conformance with required retention periods.*

There should be procedures that identify circumstances when an audit trail data file becomes full, and action should be taken to retain data as required by the retention and disposal policy.

Where an organization is working within a BS EN ISO 9001 environment, typically audit trail data relating to compliance with the quality management system are destroyed after a short period of time. This is not the case with audit trail data from information management systems, which should be stored for the same period as that of the data to which they relate.

#### 7.5.4.1.2.10 Format

*NOTE 1 The format of audit trail data is a topic often not included in information storage policies.*

*NOTE 2 Frequently, when an organization wants to automate its computer operations environment, it makes use of operating system logs to monitor the system for specific events or error conditions. At an application level, ensuring that the application provider uses standard error messages, typically agreed with the organization during the design stage, also enables application status conditions to be monitored.*

*For example, if an application reads invalid data from a file, rather than just aborting the program with nobody aware of what has happened (until the users raise a support call), the program writes a status message to an error/system log in an agreed format. The monitoring software detects this and notifies the user and/or support staff.*

Audit trail formats should enable easy interpretation, both by system users and by automated monitoring tools.

#### 7.5.4.1.2.11 Notifications

Notifications are an important trigger to investigate the continued, proper operation of the system. The entries into the error/system log that caused the monitoring software to raise the alert

should be part of the audit trail and should be controlled in accordance with BS 10008-1 and this British Standard.

#### 7.5.4.2 Date and time

Being able to determine the date and/or time of an event (such as the creation of a document by the system) can be an important piece of evidence. Thus, all appropriate events should be date- and/or time-stamped.

*NOTE 1 Depending on its importance, date and time information may be stored on a batch or individual event basis.*

Where accuracy of date and/or time clocks is important, regular checking of system clocks should be carried out. Any errors should be corrected and any actions taken documented. Only authorized personnel should be able to change system clocks. System clocks should be synchronized with an accurate time source to ensure that times recorded in audit trails are consistent and reliable.

Where clocks are changed on a seasonal basis, for example, “daylight saving summer time”, procedures to be followed should be documented.

*NOTE 2 Clock changes may be automated, but it is important to check that the appropriate action has been completed at the right time.*

In some applications, the clock can be confused by multiple time zones. Where this might be an issue, relevant procedures should be implemented to ensure that the appropriate time that ESI is accessed is recorded.

*NOTE 3 Where there is a particular need to demonstrate the accuracy of date and time stamps, the use of TTP services for this can be considered. Such services can also be used to demonstrate that system clocks have not been tampered with.*

Where trusted time (see [8.17.15](#)) is used, procedures for demonstrating the integrity and authenticity of a time stamp and its binding to a particular piece of ESI should be documented.

When information is acquired using a device, system or service outside the ESI management system, for example, mobile phone, dashboard camera, Internet of Things (IoT) device, data provider service, blockchain oracle, the ESI might contain metadata that include date and time. This metadata might be subject to different controls than the date and time stamps that are applied when the ESI is captured into the information management system. The different nature of these two sets of date and time stamps should be reviewed and the outcome of these reviews should be documented. In many cases, both sets of date and time information should be retained.

#### 7.5.4.3 Access

Access to the audit trail information should be controlled. In some applications, access might only be needed infrequently, and thus the interpretation procedures should be documented.

As audit trail data might be inspected by authorized external personnel (such as auditors) who have little or no familiarity with the system, interpretation procedures should be understandable by non-technical users.

Relevant personnel should have access to audit trail data commensurate to their role.

There should be documented procedures that are followed when audit trail data are accessed and interpreted.

There are frequently a number of departments (or individuals) within an organization or external to the organization, including those representing user, audit and legal functions, that might need access to specific parts of audit trail information. This access should be controlled, to reduce the possibility of compromise.

Access to the audit trail should itself be recorded in the audit trail.

#### 7.5.4.4 Workflow, business process management and robotic process automation

Audit trail information related to workflow, business process management (BPM) and robotic process automation (RPA) systems should be such that it includes details of any changes to workflows within specific processes, and should demonstrate the progress of specific work items through the workflow, BPM or RPA systems. Audit trail information should indicate where workers have made specific decisions, either about the ESI content or about the workflow, BPM or RPA path to be followed. A record should be created each time a new business process is defined or an existing definition is changed.

*NOTE 1 The selected audit trail points may change as the processes are changed.*

*NOTE 2 In most workflow, BPM or RPA systems, an audit trail point exists at each step in the process. However, for compliance with BS 10008-1 and this British Standard, audit trail information might not need to be kept for every audit trail point for the same retention period.*

The system should permit an authorized user to select and/or de-select the audit trail points for which audit trail data are generated. Any changes to process audit trail content should be audited.

---

## 8 Operation

### COMMENTARY ON CLAUSE 8

*This clause of this British Standard relates to BS 10008-1, Clause 8.*

*This clause gives guidance on the management of operational procedures and processes related to the storage and use of ESI.*

### 8.1 General

When responding to questions about the authenticity of managed ESI, one of the major issues organizations need to resolve relates to the requirement for proof that the system was operating correctly at all relevant times. In order to be able to deal confidently with this issue, all relevant procedural and technology issues should be well thought out, be complete in their scope, and be operated by competent individuals. Because of the long-time intervals involved, all relevant procedures should be documented.

*NOTE This documentation is described in BS 10008-1 and this British Standard as the procedures documentation and the system description documentation, which document all the operating procedures and technology that the organization needs, where appropriate, to implement.*

### 8.2 Creation

When creating digital objects within an information management system, the authenticity of the digital object should be established. Procedures for this should be documented. Where authenticity cannot be established with sufficient assurance, all appropriate information should be stored.

### 8.3 Importing

#### 8.3.1 General

Digital objects containing information might be imported into the information management system. The authenticity of these objects at the time they are imported is of critical importance when they are later called upon and their authenticity and integrity are subject to scrutiny. Hence, the authenticity of these objects should be established prior to (or as part of) the importing process.

There should be documented procedures for the importation of digital objects into the information management system. These documented procedures should include the confirmation of the integrity and authenticity of digital objects.

Where a digital object originates from outside the boundaries of control of the organization employing the information management system, there might be little or no control over, or knowledge of, the procedures or processes involved in the production or authorization of the digital object. In these circumstances, the organization should take care that the digital object and the related metadata are what they purport to be, that they have not been tampered with and that the identity of the originator is genuine.

*NOTE 1 For example, it might be important to import and verify data such as the date/time of capture, GPS coordinates and unique device identifier of a video taken using a mobile device such as a body camera, CCTV or drone system.*

*NOTE 2 The level of checking of these criteria depends upon the nature of the particular object in question and the purpose for which it was imported.*

Such boundary situations can also exist within an organization. In these circumstances, the part of the organization with the information management system should not assume that a digital object is what it purports to be, simply because it came from another part of the same organization. The organization should, again, take care that the digital object and the related metadata are what they purport to be, that they have not been tampered with and that the identity of the originator is genuine.

Digital objects can contain voice, audio and/or video information. Such digital objects should be managed in accordance with this British Standard. For all such digital objects, once the recording is frozen, the digital object should be treated in the same way as any other digital object as far as this British Standard is concerned.

Where the recording of voice, audio and/or video data is not under the control of the information management system, the recording system should have control of file integrity that is at least as good as that imposed by this British Standard for other types of information capture.

Where voice, audio and/or video data are stored, procedures for authentication of the source of the data should be documented.

### 8.3.2 Format conversion

Digital objects are typically imported directly into information management systems, either without format conversion or including a conversion to a “standard” format. Details of this importation process should be documented, along with details of any format conversions undertaken.

When importing without conversion, details of the originating software, including software name and version, should be stored. This information may be stored within the digital object or external to it. Where it is stored internally, details of how the information can be accessed should be stored.

When importing with conversion, the conversion process should be reviewed for potential loss or addition of information. Details of the conversion processes, including descriptions of any loss or addition of information, should be documented and retained.

*NOTE 1 The conversion process could, for example, lose metadata stored in the original digital object. This might happen when, for example, converting from a Microsoft Office software product to a text file format. Conversion processes might also add data, for example, to document aspects of the conversion process.*

*NOTE 2 Digital objects can be imported and stored in multiple formats. Digital objects are typically obtained from:*

- a) paper documents (originals, photocopies and faxes);*
- b) facsimile;*

- c) microfilm and microfiche;
- d) mobile devices (phones, drones, cameras, etc.); and
- e) static devices (e.g. speed cameras).

*NOTE 3 Details of procedures for capturing documents in image format are discussed in 8.5.*

*NOTE 4 Data formats store information in the original format, frequently requiring the original software to retrieve the information. There are a number of “standard” formats that can be retrieved by many software packages (e.g. text files or comma separated delimited files). Examples of data formats are:*

- a) office systems, such as those used by word processors and spreadsheets;
- b) “standard” file formats such as PDF;
- c) CAD drawings;
- d) email messages;
- e) electronic data interchange (EDI) files;
- f) HTML and web pages (intranet and internet);
- g) instant and SMS messages;
- h) Extensible Markup Language (XML) messages;
- i) video files;
- j) audio files;
- k) connected devices (e.g. IoT devices);
- l) databases and other data stores; and
- m) program to program data files.

*In all cases, the information contained in the digital object can be directly accessed by the read software.*

*NOTE 5 It is also possible to have electronic documents in mixed image and data formats (e.g. a letter in a text format with an embedded bitmapped signature).*

### 8.3.3 Dynamic data files

*NOTE 1 There are a number of data files which store data that change from time to time. The frequency of change depends upon the application, and can range from constant update (e.g. databases) to occasional update (e.g. web pages).*

Where dynamic data files are captured, the frequency and timing of the capture operation should be chosen such that all appropriate evidence is stored.

*NOTE 2 This could be either at set time intervals or prior to a change of data.*

### 8.3.4 Information loss

*NOTE 1 Whenever information is “copied”, “converted”, “moved”, “updated” or “captured” within a process, there is the potential for loss of some of the information. For example, when a photograph taken from a mobile device is reduced in size for the purpose of transferring to another device or media, resolution might be lost, resulting in the loss of detail in the picture or legibility of the document photographed. Or when an electronic document is converted from one format to another, some metadata might be lost or content layout might be changed resulting in information loss.*

*NOTE 2 In some applications, where original paper documents are scanned as part of an electronic storage system, there might be a process to destroy the original document. This process also results in information loss. In this case, the information might be the type of paper used, the ink in the pen used to sign the document or a fingerprint on the page.*