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

bsi.

Publishing and copyright information

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

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
	Foreword	**iii**
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
	Figure 1 — Encryption keys	14
	Figure 2 — Hierarchy of trust	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

Table 1 — Key recommendations 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

Annex A (normative) **Unstructured message considerations** **122**

Annex B (informative) **Application of controls** **128**
Table B.1 — Applicability matrix 130

Annex C (informative) **Example information storage policy statement** **133**

Annex D (informative) **Legal context** **135**

Annex E (normative) **Preparation of paper documents** **141**

Bibliography **157**

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, 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.[1)]

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.

1) 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.

