

BS 10008:2008



BSI Standards Publication

Evidential weight and legal admissibility of electronic information – Specification

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

Publishing and copyright information

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

© BSI 2008

ISBN 978 0 580 65119 9

ICS 03.160; 35.240.30

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

Committee reference IDT/1/3

Draft for comment 08/30172972 DC

Publication history

First published November 2008

Amendments issued since publication

Amd. no.	Date	Text affected
----------	------	---------------

Contents

Foreword *ii*

Introduction *1*

1	Scope	<i>2</i>
2	Normative references	<i>2</i>
3	Terms and definitions	<i>2</i>
4	Planning the information management system	<i>4</i>
4.1	Information management policy	<i>4</i>
4.2	Information security policy	<i>6</i>
4.3	Roles and responsibilities of workers	<i>7</i>
4.4	Reporting and communications	<i>8</i>
4.5	Documentation and records	<i>8</i>
5	Implementing and operating the information management system	<i>10</i>
5.1	Information capture	<i>10</i>
5.2	Self-modifying files	<i>12</i>
5.3	Compound documents	<i>12</i>
5.4	Version control	<i>12</i>
5.5	Information storage	<i>13</i>
5.6	Information transfer	<i>14</i>
5.7	Indexing and other metadata	<i>15</i>
5.8	Output	<i>16</i>
5.9	Identity	<i>16</i>
5.10	Disposal	<i>16</i>
5.11	Information security procedures	<i>16</i>
5.12	System maintenance	<i>18</i>
5.13	External service provision	<i>18</i>
5.14	Information management testing	<i>19</i>
6	Monitoring and reviewing the information management system	<i>20</i>
6.1	Internal audit	<i>20</i>
6.2	Management reviews	<i>20</i>
7	Maintaining and improving the information management system	<i>21</i>
7.1	Maintenance and monitoring	<i>21</i>
7.2	Preventive and corrective actions	<i>21</i>
7.3	Continual improvement	<i>22</i>

Annexes

Annex A (informative) The Plan-Do-Check-Act (PDCA) cycle *23*

Bibliography *24*

List of figures

Figure A.1 – PDCA cycle applied to information management processes *23*

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 24, an inside back cover and a back cover.



Documents

Document Sharing Hub

© BSI 2008 • 1

Foreword

Publishing information

This British Standard is published by BSI and came into effect on 30 November 2008. It was prepared by Subcommittee IDT/1/3, *General issues*, under the authority of Technical Committee IDT/1, *Document management applications*. A list of organizations represented on this committee can be obtained on request to its secretary.

Presentational conventions

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

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

Contractual and legal considerations

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

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

Introduction

BSI has published BIP 0008 (formerly PD 0008) since 1996. This code of practice has been widely adopted and is referenced, for example, by the Section 46 (61 in Scotland) Records Management Code of Practice published under the Freedom of Information Act 2000 (Freedom of Information (Scotland) Act 2002 in Scotland).

BIP 0008 now consists of the following three parts:

- BIP 0008-1, *Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008*;
- BIP 0008-2, *Evidential weight and legal admissibility of information transferred electronically – Code of practice for the implementation of BS 10008*;
- BIP 0008-3, *Evidential weight and legal admissibility of linking electronic identity to documents – Code of practice for the implementation of BS 10008*.

This British Standard covers the scope of all three parts of BIP 0008. Its publication reflects the requests of the adopters of BIP 0008 for a formal compliance standard.

The detailed guidance given in the latest edition of BIP 0008 will assist in the successful implementation of this British Standard.

If a corporate body's electronic information management system conforms to this British Standard, it is anticipated that the evidential weight of electronic information managed by the corporate body will be maximized, by ensuring its trustworthiness and reliability. It is also anticipated that conformity with this British Standard will minimize the risks involved with the long-term storage of information in an electronic form.

This British Standard has been structured along the lines of the Plan-Do-Check-Act model (PDCA) used in the majority of management system standards, as a model for continual improvement. An outline of the PDCA model is given in Annex A.

1 Scope

This British Standard specifies requirements for the implementation and operation of electronic information management systems, including the storage and transfer of information, and addresses issues relating to the authenticity and integrity of the information. These issues are important where the information might be used as evidence.

This British Standard covers:

- the management of the availability of electronic information over time;
- electronic identity verification, including the use of electronic signatures and electronic copyright systems, as well as the linking of electronic identity to particular electronic information.

It does not cover processes used to evaluate the authenticity of information prior to it being captured in the system.

The requirements specified in this British Standard are generic and intended to be applicable to all corporate bodies (or parts thereof), regardless of type, size and nature of business. The extent of application of these requirements depends on the corporate body's operating environment and complexity.

This British Standard applies to electronic information in any form.

NOTE 1 The form of the information might be "office type" documents (such as word processed documents, spreadsheets, presentations), electronic images or databases. The information might also contain 3-dimensional images or voice/video recordings.

NOTE 2 Annex A gives information on the PDCA model.

2 Normative references

The following referenced document is indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS ISO 12651, *Electronic imaging – Vocabulary*

3 Terms and definitions

For the purposes of this British Standard the terms and definitions given in BS ISO 12651 and the following apply.

3.1 compound document

information constructed from a number of separate digital documents

3.2 conversion

translation of electronic information from one file format to another

3.3 corporate body

organization or group of persons that is identified by a particular name and that acts, or can act, as an entity

3.4 document

information stored on media

[BIP 0008]

3.5 electronic image

electronic bit-mapped representation of a physical (e.g. paper or microfilm) document

3.6 information management

processing and storage of information in a controlled manner

3.7 metadata

data about data

[BIP 0008]

3.8 migration

transfer of electronic information from one storage media to another

NOTE This might or might not involve the removal from the original storage media.

3.9 nonconformity

non-fulfilment of a requirement

[BS EN ISO 9000; BS EN ISO 14001]

3.10 policy

deliberate plan of action to guide decisions and achieve rational outcome(s)

3.11 procedure

documented set of actions which is the official or accepted way of doing something

3.12 process

series of actions taken in order to achieve a result

3.13 record

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

[BS ISO 15489-1]

3.14 system

electronic system which stores and/or processes information in a digital or analog form

[BIP 0008]

3.15 workers

individuals working under the control of a corporate body, including employees, temporary staff, contractors and consultants

4 Planning the information management system

4.1 Information management policy

Objective: To provide direction and support for the management of electronic information.

4.1.1 General

The corporate body's senior management team shall set a clear policy direction and demonstrate support for, and commitment to, the management of the electronic information through the issue and maintenance of an information management policy.

NOTE The senior management team might consist of the Board of Directors, the Chief Executive and his/her senior staff, the partners or the owner of a sole trader company.

The policy shall cover:

- a) the storage of electronic information over time (see 4.1.2);
- b) the transfer of electronic information between systems (see 4.1.3).

The policy shall be linked to or shall be combined with the corporate body's information security policy (see 4.2).

The policy shall be published and communicated to all appropriate workers.

The policy shall have a custodian, who is responsible for its maintenance and review in accordance with the corporate body's approved review procedure (see 4.1.4).

4.1.2 Electronic storage policy statement

The electronic storage policy document shall state management's commitment to, and approach for, the use of electronic systems in the storage of information over time in a controlled manner, bearing in mind the need to retain maximum evidential weight.

The policy statement shall include the following elements or, where applicable, reference separate documentation on:

- a) the scope of the policy;
- b) the application of any applicable security classification to individual documents;
- c) the implementation of various British and International Standards and industry-related requirements and guidelines;
- d) any consultations that the corporate body needs to undertake (see 4.1.5);
- e) the definition and allocation of roles and responsibilities for information storage (see 4.3);
- f) the use of the appropriate electronic storage technology (see 5.5.2);
- g) the use of the appropriate electronic file formats (see 5.5.4);

- h) the management of the linking of electronic identity to information (see **5.9**);
- i) the retention and disposal of information (see **5.10**);
- j) the auditing of the information management system (see **6.1**).

NOTE Other elements may be included.

4.1.3 Electronic transfer policy statement

The electronic transfer policy document shall state management's commitment to, and approach for, the use of electronic systems for the transfer of information in a controlled manner, bearing in mind the need to retain maximum evidential weight.

The policy statement shall include the following elements or, where applicable, reference separate documentation on:

- a) the scope of the policy (which might be different from that for electronic storage);
- b) the definition and allocation of roles and responsibilities for information transfer (see **4.3**);
- c) the communication of specific types of information;
- d) the use of data compression;
- e) the use of particular systems for the transfer of electronic information (see **5.6**);
- f) the receiving of transferred electronic information;
- g) the management of the linking of electronic identity to information (see **5.9**);
- h) the use of encryption (see **5.11.3**);
- i) the auditing of the information management system (see **6.1**).

NOTE Other elements may be included.

4.1.4 Review and evaluation

A procedure shall be established to ensure that the policy is reviewed at regular intervals, and when any significant changes occur to the appropriate business, legal and/or regulatory environment.

4.1.5 Legal and regulatory environment

Consultations shall be undertaken to identify any nonconformity with appropriate legal and/or regulatory requirements relevant to the information management system.

The outcomes of these consultations and actions taken to resolve any nonconformity shall be logged.

4.2 Information security policy

Objective: To ensure that the information management system is operated in accordance with the approved information security policy.

4.2.1 General

The corporate body shall ensure that the information management system operates within the corporate body's information security policy.

The security policy shall cover:

- a) the storage of electronic information over time (see 4.2.2);
- b) the transfer of electronic information between systems (see 4.2.3).

NOTE BS ISO/IEC 27001 is the UK reference document for information security management. When its requirements are implemented within the boundaries of BS 10008, it can provide helpful supporting evidence of the authenticity and integrity of the electronic information.

4.2.2 Storage security policy statement

Where electronic storage of information over time is undertaken, the information security policy shall include the following elements, or shall reference separate documentation, regardless of whether conformity with BS ISO/IEC 27001 is a requirement of this policy:

- a) the scope of the policy;
- b) the management objectives relating to the security of stored electronic information;
- c) the security requirements for different information classification categories;
- d) the definition and allocation of roles and responsibilities for information security management (see 4.3);
- e) the segregation of roles, to address the risk of either accidental or malicious changes to, or disclosure of, information;
- f) access rights and the sharing of information (see 5.11.2);
- g) procedures for dealing with actual or suspected security breaches;
- h) the need for conformity with any information security standards adopted, such as BS ISO/IEC 27001;
- i) the review and updating of the policy.

NOTE Other elements may be included.

4.2.3 Transfer security policy statement

Where electronic transfer of information is undertaken, the information security policy shall include the following elements, or shall reference separate documentation, regardless of whether conformity with BS ISO/IEC 27001 is a requirement of this policy:

- a) the scope of the policy (which might be different from that for electronic storage);
- b) the management objectives relating to the security of electronic information during transfer;