BS 10008:2008

BRITISH STANDARD

Evidential weight and legal admissibility of electronic information – Specification

ICS 03.160; 35.240.30

Publishing and copyright information

ISBN 978 0 580 65119 9

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

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.

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;

c) the security requirements for different information classification categories;

d) the definition and allocation of roles and responsibilities for information security management related to the electronic transfer of information (see **4.3**);

e) the segregation of roles, to address the risk of either accidental or malicious changes to, or disclosure of, information;

f) procedures for dealing with actual or suspected security breaches during electronic information transfer;

g) the management and application of electronic identity linked to information (see **5.9**);

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.

4.2.4 Risk assessment

The information security policy shall be based on the results of an information security risk assessment, covering all identified risks to the authenticity, integrity and availability of the stored and/or transferred information.

NOTE Compliance with BS ISO/IEC 27005 should be considered when identifying, evaluating, treating and managing information security risks.

4.3 Roles and responsibilities of workers

The corporate body shall define and document the roles and responsibilities needed to establish, implement, operate and maintain the information management system.

Senior management shall:

a) appoint or nominate a person with appropriate seniority and authority to be accountable for the information management policy and its implementation;

b) appoint one or more persons, who, irrespective of other responsibilities, shall implement and maintain the information management system.

NOTE For a small corporate body, responsibility for the information management system may be taken by a single individual as part of a job portfolio. In larger corporate bodies, an individual with this responsibility should be clearly identified.

The individual or team with responsibility for managing the system shall:

1) follow a systematic and organized approach to monitoring known conformity issues and recommending appropriate action;

2) be business-focused and aware of the current state of the business and its priorities;

3) be able to communicate at all levels within the corporate body;

4) have a good understanding of the risks involved should the authenticity, integrity and/or availability of the information be compromised.

4.4 Reporting and communications

A communication plan shall be established which identifies:

a) mechanisms for disseminating decisions;

b) mechanisms for collecting feedback;

c) mechanisms for the regular updating of risk information;

d) procedures for dealing with challenges to the authenticity and/or integrity of information being used as evidence;

e) key individuals within the corporate body responsible for managing such communications.

4.5 Documentation and records

Objective:

a) To ensure that adequate documentation of implemented procedures and technology is available for user reference, training purposes and procedural audits, and for future use as evidence.

b) To enable the demonstration that the information management system is operating in accordance with policy and procedures.

4.5.1 General

The corporate body shall have documentation covering the following aspects of the information management system:

a) the information management and information security policies (see **4.1** and **4.2)**;

b) risk assessment (see **4.2.4**);

c) the roles and responsibilities of personnel (see **4.3)**;

d) reporting and communications (see **4.4**);

e) system procedures (see **4.5.2**);

f) the key technology components (see **4.5.3**);

g) all activities carried out in relation to the information management system in the form of audit trails (see **4.5.4**);

h) internal audit reporting (see **6.1**);

i) management review (see **6.2**);

j) maintenance and monitoring (see **7.1**);

k) preventive and corrective actions (see **7.2**);

l) continual improvement (see **7.3**).

Records shall be established, maintained and controlled to provide evidence of the effective operation of the information management system.

Procedures shall be established to identify the controls over documentation.

Responsibility for overseeing the management of documentation shall be clearly assigned and agreed.

4.5.2 Procedures manual

A manual shall be produced, detailing the procedures to be followed relating to the information management system.

NOTE 1 The "information management system" includes all technology (hardware and software) related to the information management processes.

Where a quality management system is in operation, the manual shall conform to the requirements of that system.

The manual shall:

a) have an owner;

b) be reviewed on a regular basis;

c) be updated to describe actual processes as and when they are implemented.

Superseded versions of the manual shall be retained in accordance with the corporate body's retention policy.

NOTE 2 Documentation should be retained for at least as long as the information to which it relates.

4.5.3 System description

A description of the key technology components used for the electronic information management system shall be produced.

NOTE 1 "Technology" includes software and hardware.

Where a quality management system is in operation, this documentation shall conform to the requirements of that system.

The system description shall:

a) have an owner;

b) be reviewed on a regular basis and after a significant change to the technology;

c) be updated to describe the implemented technology.

Superseded versions of the system description shall be retained in accordance with the corporate body's retention policy.

NOTE 2 Documentation should be retained for at least as long as the information to which it relates.

4.5.4 Audit trails

4.5.4.1 General

Audit trails shall be created, containing information which enables the sequence and details of activities related to the information management system to be determined.

Audit trails shall show activities related to:

a) the information management system;

b) the stored information;

c) the transferred information.

NOTE 1 Audit trails should be designed to meet the audit requirements detailed in PD 0018.

*NOTE 2 It is recommended that additional audit trails are created to document and/or manage the processes related to migration and conversion (see **5.5.3** and **5.5.5**).*

Audit trails shall be included in the retention schedule and audit trail information shall be retained for at least as long as the information to which it relates.

4.5.4.2 Date and time

Where the date and/or time of an event is relevant, appropriate timing data shall be stored in association with the event in the audit trail. The accuracy of the timing data, and its relationship with any external time systems, shall be demonstrable.

4.5.4.3 Access

Access to audit trail information shall be controlled to maintain its integrity. This access shall be on a read-only basis. A procedure for reviewing the information contained in audit trails shall be established to ensure that the audit trail information can be interpreted by users and by system auditors.

Access to the audit trail shall be recorded as an entry in the audit trail.

4.5.5 Workflow

Where workflow capabilities are used as part of the information management process, audit trail information shall give details of the following:

a) any additions or changes to the workflow process;

b) the progress of any work item through the workflow.

5 Implementing and operating the information management system

5.1 Information capture

Objective: To ensure that any information loss occurring as a result of the capture processes is acceptable to the corporate body.

5.1.1 General

Procedures shall be established for the capture of information, created either outside or within the information management system, to ensure that any information loss as a result of the capture processes is acceptable to the corporate body.

Where digital objects contain data that might change periodically (e.g. a corporate website), the frequency and timing of capture of updated digital objects shall be specified.

Capture procedures shall be such as to ensure that necessary information is in fact captured.

5.1.2 Importing

Importing procedures shall be established such that, where information has been created in an electronic form (e.g. as a digital object) outside the information management system, it is imported into the system in a manner acceptable to the corporate body.

Importing procedures shall be such as to ensure that:

a) digital objects are captured without change, or in association with a file format change;

b) there is a log of imported digital objects;

c) all associated metadata is imported in conjunction with the imported digital object.

5.1.3 Document scanning

Where scanning technology is used, procedures shall be established for the scanning of documents in paper form, microforms and other forms of information, as appropriate. These procedures shall be such as to ensure that any potential information loss due to the scanning processes is within acceptable limits.

*NOTE 1 In some information management systems, document scanning is considered as part of the information management system. In other systems, separate document scanning systems create electronic images that are subsequently imported into the system (see **5.1.2**).*

Quality control procedures shall be established to check for missing images and/or images that do not meet specified quality standards.

NOTE 2 Scanner test targets as specified in BS ISO 12653-1 should be used as a test of scanner quality. The procedures specified in BS ISO 12653-2 should be used as a basis for these tests. The results of these tests should be retained in the information management system in line with the corporate body's retention policy.

Rescanning procedures shall be established to correct any errors identified, as far as possible.

Where rescanning is not possible, or would result in a new image of equal or poorer quality, the original image shall be identified as best achievable quality.

NOTE 3 The relevant quality issue should be indicated on the identification.

Where batching techniques are used in scanning, numbers shall be allocated to each batch. Associated scanning information (e.g. time, date, scanner number, number of pages) shall be created and retained.

NOTE 4 The appropriate batch number should be recorded in the metadata associated with each electronic image.

Where documents in paper form are photocopied and the photocopies scanned, the images shall be identified as being from photocopies.

5.1.4 Data extraction

Where data is extracted from image files (e.g. using optical character recognition (OCR) or bar code recognition), the original images shall be retained and linked with the captured data.

5.1.5 Metadata capture

Metadata shall be captured to ensure that details of the information capture processes are retained throughout the storage life of the information.

Procedures for the capture of all metadata required to meet business requirements shall either be part of, or shall be linked to, the information capture procedure.

5.2 Self-modifying files

Objective: To ensure a consistent rendering of information throughout its storage life.

Executable code or other mechanisms embedded in data files shall be avoided, wherever possible, as these can result in the amendment of displayed/printed forms of the information or, occasionally, of the stored information.

NOTE One method of avoiding the effects of such code is to convert to a file format that does not support this feature. Such conversion should be such as to ensure that the converted file retains the original information.

5.3 Compound documents

Objective: To ensure that all the components of a document that comprises more than one digital object (typically managed by links from one object to another) are retained.

Where information in the form of a compound document is stored, the linkage of all elements of the compound document shall be stored in line with the retention policy along with their content.

5.4 Version control

Objective: To ensure that the latest version of any document is identified as such, and is made available on request.

Where stored information can be amended periodically, an appropriate version control procedure shall be established to ensure that superseded versions of stored information are retained in accordance with the retention schedule.

Version control procedures shall also ensure that the latest version of the stored information is accessed, unless a previous version is specifically requested.

5.5 Information storage

Objective:

a) To ensure that information stored in an electronic form is retained in accordance with the corporate body's retention schedule.

b) To ensure that, where retention periods are longer than the anticipated life of the storage technology (including software and hardware), procedures are established which retain the information, without compromise to authenticity and integrity.

5.5.1 General

Procedures shall be established to demonstrate that stored information has not been changed (either accidentally or maliciously) or, where changes have occurred, they have been authorized during storage.

Information shall be retained for no longer than its retention period unless:

a) the information is required to support existing and/or anticipated litigation;

b) there is an external reason for longer retention.

Where information is compressed during the storage process (e.g. in order to reduce stored file size), the compression methods used shall not affect the authenticity and integrity of the stored information.

5.5.2 Storage technology

Storage technology shall be chosen in accordance with the information management policy (see **4.1**).

Storage technology shall be installed and operated in accordance with manufacturer's recommendations. Where removable storage media is used, it shall be handled and stored in accordance with manufacturer's recommendations.

Procedures shall be established to test storage media at regular intervals to reduce the risk of unrecoverable errors.

5.5.3 Migration

When information is migrated to new storage media, procedures shall be established to ensure that:

a) all appropriate digital objects have been migrated to the new storage technology;

b) the file format of the migrated digital objects has not changed (but see conversion (**5.5.5**), which might take place at the same time as a migration procedure);

c) the digital objects themselves have either not been changed or the changes are known, audited and meet the corporate body's requirements.

NOTE Techniques such as audit trails and checksums should be used to document and/or manage the processes used.

5.5.4 Storage file formats

Information shall be stored and maintained in a file format that is predicted to allow access over the relevant retention period.

*NOTE The storage file formats selected might be such that conversion to newer file formats is required (see **5.5.5**). Alternatively, the storage file format might be such that access can be achieved over the long term. There could be an advantage in selecting file formats that have been developed for long-term preservation and that conform to International Standards, such as BS ISO 19005-1 (Use of PDF/A).*

5.5.5 Conversion

Where replacement software (e.g. an operating system or application software) is implemented, procedures shall be established, where necessary, to retain access to the stored information.

Where file format conversion is used, the procedures established shall be such as to demonstrate that all appropriate digital objects have been converted to the new software systems, and that the information contained within the digital objects retains its authenticity and integrity.

NOTE 1 Audit trails should be used to document the processes used.

NOTE 2 Where file format conversion is used, the converted information should be retained in both the original and the new file formats.

5.6 Information transfer

Objective: To ensure that electronic transfer processes are managed in accordance with the information transfer policy.

5.6.1 General

When electronic information is transferred between systems, procedures shall be established covering the:

a) preparation of an electronic file and all appropriate metadata for transfer;

b) management and elimination, where possible, of malicious software;

c) use of file compression and decompression techniques;

d) use of file encryption and decryption techniques, and the management of cryptographic keys;

e) application and verification of sender/recipient identity;

f) use of digital signatures and other file integrity demonstration systems;

g) conversion to alternative file format prior to transmission;

h) selection of the appropriate communications system for the transfer;

i) initiation of a transfer;

j) receipt of a transfer;

k) conversion to an alternate format on receipt;

l) use of “confirmation of receipt” messages.

5.6.2 Transmission

Where stored information is electronically transferred between systems, the transfer shall be such that the integrity of the information is not compromised during transfer (including during initiation and receipt/storage).

All appropriate metadata shall be transmitted in association with the transferred information.

Details of the transfer processes used shall be retained for as long as the information to which they relate.

5.6.3 Message transmission systems

Where message transmission systems are used (e.g. email, SMS messages), to ensure that the integrity of the information is not compromised during message transmission, procedures shall be established covering the:

a) titling and addressing of messages;

b) standards for drafting (including language, jargon and other message content);

c) use of spellcheckers and other message checking tools;

d) use of passwords, digital signatures and other content management tools;

e) use of "copy-to" and "blind copy-to";

f) detection and elimination of malicious software;

g) inclusion of attachments and embedded links;

h) use for legal purposes such as contracts;

i) avoidance of breach of copyright;

j) accuracy in content and addressing where electronic business is conducted;

k) management of and response to messages on receipt.

5.7 Indexing and other metadata

Objective: To ensure that all stored information can be located in a timely manner at any time during its storage life.

Where indexes are used, stored information shall be indexed in a manner that facilitates future retrieval.

Wherever appropriate and practical, indexing shall be automated.

Indexing metadata shall be retained for at least as long as the information to which it relates.

Indexing error correction procedures shall be established and shall include an audit trail which identifies the information being corrected and the individual making the correction.

NOTE For further details of metadata capture, see BS ISO 23081-1 and DD ISO/TS 23081-2.

5.8 Output

Objective: To ensure that information can be produced in an authenticated form when required for evidential purposes.

Procedures shall be established for the output of stored information in a human-readable or human-interpretable form, as appropriate.

Where output is required as evidence in legal or other proceedings, procedures for certifying that the output is authentic shall be used.

5.9 Identity

Objective: To ensure that the identity of the parties involved in information capture and transfer is authentic.

Where the identity of those involved in information capture or transfer is important, procedures which authenticate the identity of the person, corporate body or other entity shall be established.

These procedures shall be such as to ensure that:

a) the authenticated identity is bound to the electronic information;

b) the processes used for proof of identity are retained, along with their results.

5.10 Disposal

Objective: To ensure that information is disposed of in a secure manner in accordance with the corporate body's retention and disposal policy.

Information disposal procedures shall be established that are in accordance with the corporate body's information security policy (see **4.2**).

Information shall be disposed of at the end of its retention period, in accordance with the corporate body's disposal policy [see **4.1.2**, item i)].

Information shall be retained in audit trails, or using other appropriate processes, which record the disposal of information as specified in the retention and disposal policy.

5.11 Information security procedures

Objective:

a) To ensure that the information management system is operated in accordance with the information security policy.

b) To ensure that electronic information is protected from accidental or deliberate loss during storage and/or transfer.

5.11.1 General

The corporate body shall establish procedures for ensuring that the information management system is operated in accordance with the information security policy (see **4.2**).

5.11.2 Access rights

Access to information and/or indexing and other metadata shall be controlled using appropriate authentication and authorization procedures, such that only workers with the appropriate permissions can:

a) access information (e.g. without the allocation of enter/amend/delete rights when read-only access is required);

b) enter new information;

c) amend information;

d) delete information.

Where access is required by support and/or maintenance workers, it shall be approved, controlled and audited.

All access to information and/or indexing and other metadata shall be audited, where appropriate.

5.11.3 Encryption

Where information is stored and/or transferred in an encrypted form, cryptographic keys and algorithms shall be managed in accordance with the information security policy.

Where encrypted information is retained, the ability to access digital certificates, signature keys and algorithms to enable the encrypted information to be decrypted shall be maintained for as long as the encrypted information is retained.

5.11.4 Digital signatures

Where digital signatures or other authentication techniques are used, access to digital certificates, signature keys and algorithms shall be controlled in accordance with the information security policy.

Where digital signatures are retained, the ability to validate digital certificates and to access digital certificates, signature keys and algorithms to enable the digital signatures to be validated shall be maintained for as long as the digitally signed information is retained.

5.11.5 Back-up and recovery

Procedures shall be put in place that protect electronic information during storage and/or transfer from loss or corruption (actual or suspected).

NOTE Such procedures are typically included in the corporate body's backup and recovery strategy.

The back-up and restore/recovery procedures shall be tested at regular intervals to ensure that recovery can be achieved in the event of an information loss (see also **5.14**).

Details of all recovery operations shall be retained for as long as the information to which they relate.

5.11.6 Business continuity planning

The corporate body shall develop procedures to be implemented in the event of an actual or suspected disaster related to the information management system. Disasters to be included in the procedures shall include those related to the interruption of services, to natural causes and to human intervention.

Business continuity plans shall be tested on a regular basis, and the results of the tests documented. Where tests demonstrate that the plans need to be modified to meet business needs, the plans shall be modified and re-tested.

Where business continuity plans have been implemented in relation to an operational information management system, a report on the success or otherwise of the recovery shall be produced. This report shall detail any actual or suspected compromise to the authenticity, integrity and/or availability of the related electronic information.

NOTE BS 25999-1 and BS 25999-2 give details of business continuity management systems.

5.12 System maintenance

Objective: To ensure that equipment operates in a reliable manner, by maintaining the system in accordance with the manufacturer's recommendations.

All hardware and software components of the information management system that require systematic maintenance shall be maintained in accordance with the manufacturer's recommendations.

A record of system maintenance shall be retained in accordance with the retention policy.

5.13 External service provision

Objective: To ensure that the authenticity, integrity and availability of electronic information during storage and/or transfer are not compromised as a result of the use of an external service provider.

NOTE 1 Service providers may be located within the corporate body's premises (insourced) or at another location (outsourced).

NOTE 2 Attention is drawn to the fact that some functions are required by legal and/or regulatory requirements to be performed within or by the corporate body.

5.13.1 Procedures

Where an external service provider is used, the corporate body shall specify those actions to be taken by the service provider to enable the corporate body to continue to demonstrate compliance with its information management and information security policies.

5.13.2 Compliance

Where a service provider claims compliance with this British Standard, the corporate body shall require that proof of compliance be demonstrated on request and at regular intervals through the appropriate management of audit trail information.

NOTE This might involve the provision of a copy of the audit trail, secure storage of the audit trail or the provision of access to the audit trail.

5.13.3 Security in transfer

The corporate body shall specify the security requirements for information whilst in transit between the corporate body and the service provider (whether this is by electronic or physical means).

NOTE Where information technology services are involved, compliance with BS ISO/IEC 20000-1 should be considered.

5.13.4 Overseas

Where overseas service provision is used, the corporate body shall specify that all applicable UK legislative requirements relating to the management of information are to be met.

5.14 Information management testing

Objective: To verify the ongoing effectiveness of the information management system.

The corporate body shall test its information management system to ensure that it meets business requirements.

The corporate body shall:

a) develop tests that are consistent with the scope of the information management system;

b) have a programme approved by senior management to ensure that testing is carried out at planned intervals and when significant changes occur;

c) carry out a range of different tests that taken together validate the whole of its information management system;

d) plan tests so that the risk of an incident occurring as a direct result of the test is minimized;

e) define the aims and objectives of every test;

f) carry out a post-test review of each test that will assess the achievement of the aims and objectives of the test;

g) produce a written report of the test, outcome and feedback, including required actions.

6 Monitoring and reviewing the information management system

Objective: To ensure that the effectiveness and efficiency of the information management system is monitored and reviewed.

6.1 Internal audit

6.1.1 Audit requirements

Audits shall be conducted at planned intervals to determine whether the information management system:

a) is effective in meeting the corporate body's information management policy (see **4.1**);

b) is operating in accordance with the policy and established procedures;

c) has been implemented and maintained in accordance with technology requirements.

Audit results shall be provided based on the requirements of the corporate body.

6.1.2 Audit planning

An audit programme shall be planned, established and maintained by the corporate body, taking into account the information management and information security policies.

6.1.3 Audit procedures

Audit procedures shall be established that address:

a) the responsibilities, competencies and requirements for planning and conducting audits, reporting results and retaining associated records;

b) the determination of audit criteria, scope, frequency and methods.

6.1.4 Selection of auditors

The selection of auditors and the conduct of audits shall be such as to ensure objectivity and the impartiality of the audit process.

6.2 Management reviews

A management review of the information management system shall be carried out at regular, scheduled intervals, and when major changes take place, to ensure the system's continuing suitability, adequacy and effectiveness.

The management review shall be based on:

a) feedback from users of the information management system;

b) the results of audits;

c) records of procedural reviews;

d) records of technology modifications.

The results of the management review shall provide detailed information about changes to the information management system.

NOTE Detailed information might be the identification of modifications to procedures and/or technology that might affect the authenticity, integrity and/or availability of the stored and/or transferred information.

7 Maintaining and improving the information management system

Objective: To maintain and improve the effectiveness and efficiency of the information management system, by ensuring that issues identified during an audit, management review or ongoing operations are addressed and suitable amendments made to policy and/or technology.

7.1 Maintenance and monitoring

Implemented processes shall be regularly monitored and reviewed to ensure that they are operating in accordance with the appropriate procedures, and that changes in the corporate body's requirements and/or technology have not compromised the authenticity, integrity and/or availability of the information.

The majority of procedures and technology components will require maintenance and administrative support to ensure their correct and appropriate functioning during their life; these activities shall be planned and performed on a regular, scheduled basis.

Maintenance activities shall include at least the following:

a) the checking of audit trail and log files;

b) the modification of procedures to reflect changes and additions;

c) the reviewing of compliance with procedures.

7.2 Preventive and corrective actions

7.2.1 General

The corporate body shall improve the information management system through the application of preventive and corrective actions.

All proposed changes and/or improvements shall be assessed prior to implementation to ensure that the requirements of the information management and information security policies are met.

Where major changes are implemented, an audit shall be completed as soon as possible after implementation. Where changes that might affect the integrity of the stored information take place (such as a migration to new storage media and/or a conversion to a new storage file format), the change procedure itself shall be audited.

Changes arising from preventive and corrective actions shall be documented and retained in accordance with the retention schedule.

7.2.2 Preventive actions

The corporate body shall take action to guard against potential nonconformities in order to prevent their occurrence. A procedure shall be established for:

a) identifying potential nonconformities and their causes;

b) determining and implementing preventive action needed;

c) recording results of, and reviewing, action taken;

d) identifying changed risks;

e) ensuring that all those who need to know are informed of the potential nonconformity and the preventive action put in place.

7.2.3 Corrective actions

Where items of nonconformity are identified, a procedure shall be established for reviewing each item and, based on a risk assessment, either:

a) eliminating the cause of the nonconformity;

b) reducing the level of nonconformity; or

c) where the risk assessment determines that a reduction in the level of nonconformity is not warranted, documenting this position in detail.

The risk assessment shall be conducted at regular intervals to determine whether the position has changed and the nonconformity needs to be rectified.

7.3 Continual improvement

The corporate body shall seek to continually improve the effectiveness of the information management system through the review of the information management policy, audit results, preventive and corrective actions, and management review.

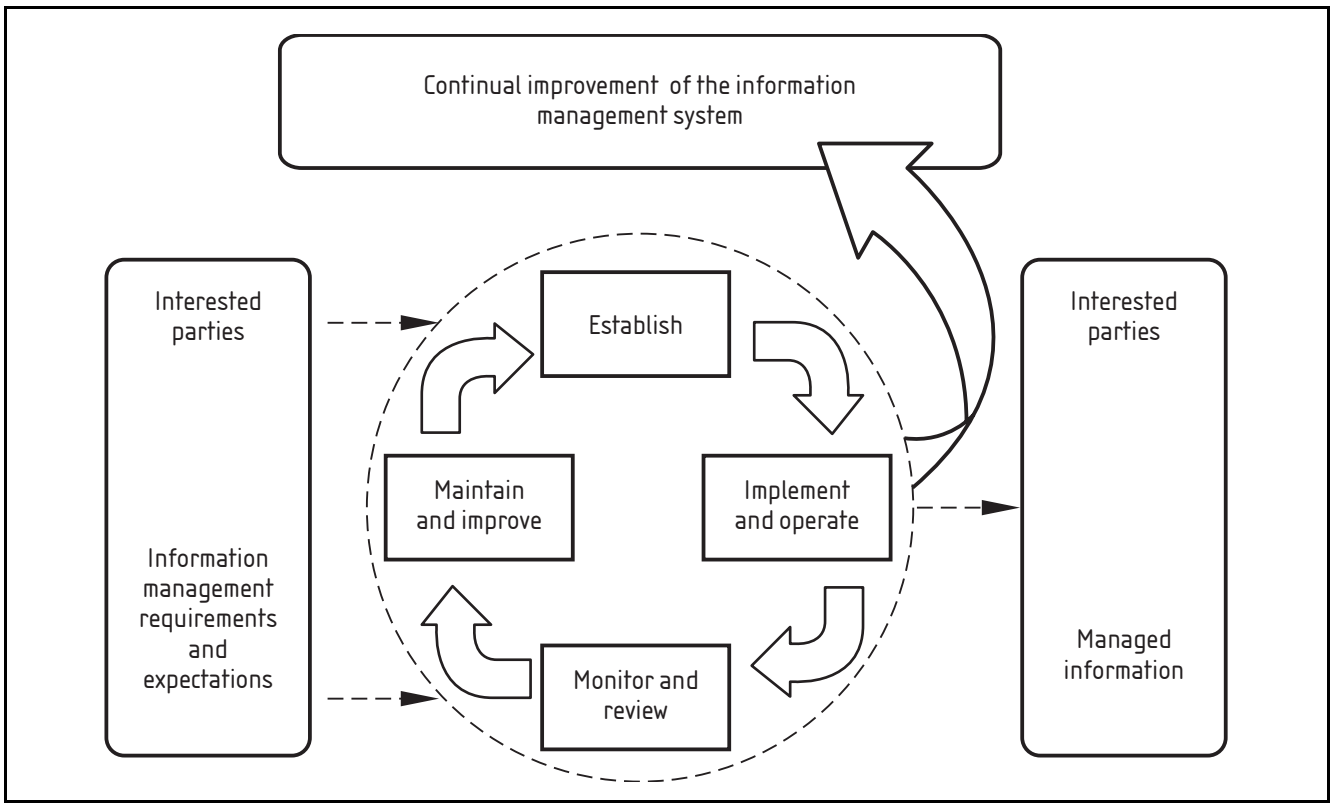
Annex A (informative) The Plan-Do-Check-Act (PDCA) cycle

This British Standard applies the "Plan-Do-Check-Act" (PDCA) cycle to establishing, implementing, operating, monitoring, exercising, maintaining and improving the effectiveness of a corporate body's information management system. This ensures a degree of consistency with other management systems standards, thereby supporting consistent and integrated implementation and operation with related management systems. Other management systems standards include:

- BS EN ISO 9001 (Quality management systems);
- BS EN ISO 14001 (Environmental management systems);
- BS ISO/IEC 20000 (IT service management);
- BS ISO/IEC 27001 (Information security management systems).

Figure A.1 illustrates how an information management system takes as inputs the various requirements of this British Standard and, through the necessary actions and processes, produces information management outcomes (i.e. managed information) that meet those requirements.

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



Plan	To establish direction and support for the management of electronic information.	Clause **4**
Do	To implement and operate the information management policy, processes and procedures.	Clause **5**
Check	To monitor and review the effectiveness and efficiency of the information management system, by undertaking internal audits and management reviews.	Clause **6**
Act	To maintain and improve the effectiveness and efficiency of the information management system, by ensuring that issues identified during an audit or ongoing operations are addressed and suitable amendments made to policy and/or technology.	Clause **7**

Bibliography

BS 25999-1, *Business continuity management – Part 1: Code of practice*

BS 25999-2, *Business continuity management – Part 2: Specification*

BS EN ISO 9001, *Quality management systems – Requirements*

BS EN ISO 14001, *Environmental management systems – Requirements with guidance for use*

BS ISO 12653-1, *Electronic imaging – Test target for the black-and-white scanning of office documents – Part 1: Characteristics*

BS ISO 12653-2, *Electronic imaging – Test target for the black-and-white scanning of office documents – Part 2: Method of use*

BS ISO 15489-1, *Information and documentation – Records management – Part 1: General*

BS ISO 19005-1, *Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)*

BS ISO/IEC 20000-1, *Information technology – Service management – Part 1: Specification*

BS ISO 23081-1, *Information and documentation – Records management processes – Metadata for records – Part 1: Principles*

BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

BS ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*

DD ISO/TS 23081-2, *Information and documentation – Records management processes – Metadata for records – Part 2: Conceptual and implementation issues*

PD 0018, *Information management systems – Building systems fit for audit*

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

BIP 0008-2, *Evidential weight and legal admissibility of information transferred electronically – Code of practice for the implementation of BS 10008*[1)]

BIP 0008-3, *Evidential weight and legal admissibility of linking electronic identity to documents – Code of practice for the implementation of BS 10008*[1)]

1) Due for publication in late 2008.

This page deliberately left blank

BSI – British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.
Tel: +44 (0)20 8996 9000 Fax: +44 (0)20 8996 7400

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001
Fax: +44 (0)20 8996 7001 Email: orders@bsigroup.com

You may also buy directly using a debit/credit card from the BSI Shop on the Website http://www.bsigroup.com/shop.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111
Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002
Fax: +44 (0)20 8996 7001 Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsigroup.com/BSOL.

Further information about BSI is available on the BSI website at http://www.bsigroup.com.

BSI Group Headquarters
389 Chiswick High Road,
London W4 4AL, UK
Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

Copyright