

Evidential weight and legal admissibility of electronic information – Collection



Peter Howes and Alan Shipman

Evidential weight and legal admissibility of electronic information – Collection

Peter Howes and Alan Shipman

bsi.

First published 2015

by

BSI Standards Limited
389 Chiswick High Road
London W4 4AL

© The British Standards Institution 2015

All rights reserved. Except as permitted under the Copyright, Designs and Patents Act 1988, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior permission in writing from the publisher.

Whilst every care has been taken in developing and compiling this publication, BSI accepts no liability for any loss or damage caused, arising directly or indirectly in connection with reliance on its contents except to the extent that such liability may not be excluded in law.

While every effort has been made to trace all copyright holders, anyone claiming copyright should get in touch with the BSI at the above address.

BSI has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this book, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

The rights of Peter Howes and Alan Shipman to be identified as the authors of this Work have been asserted by them in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

Typeset in Great Britain by Letterpart Limited, www.letterpart.com

Printed in Great Britain by Berforts Group, www.berforts.co.uk

British Library Cataloguing in Publication Data

A catalogue record for these books is available from the British Library

ISBN 978 0 580 89211 0

BIP 0142

Foreword

Evidential Weight and Legal Admissibility of Electronic Information - Collection

This collection comprises

- BS 10008:2014, *Evidential weight and legal admissibility of electronic information — Specification*
- 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 information documents – Code of practice for the implementation of BS 10008*
- BIP 0009, *Evidential weight and legal admissibility of electronic information - Compliance workbook for use with BS 10008:2014*

BS 10008:2014



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.

© The British Standards Institution 2014

Published by BSI Standards Limited 2014

ISBN 978 0 580 83673 2

ICS 03.160; 35.240.30

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

Committee reference IDT/1

Draft for comment 14/30286703 DC

Publication history

First published November 2008

Second (present) edition, December 2014

Amendments issued since publication

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

Contents

Foreword 1

Introduction 2

1 Scope 4

2 Normative references 4

3 Terms and definitions 4

4 Context of the organization 6

5 Leadership 7

6 Planning 12

7 Support 13

8 Operation 16

9 Performance evaluation 25

10 Improvement 27

Bibliography 28

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 30, an inside back cover and a back cover.



Documents

© The British Standards Institution 2014 [Documents](#) [Sharing Hub](#)

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 08 December 2014. It was prepared by Panel IDT/1/-/5, *Legal admissibility*, 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.

Supersession

This British Standard supersedes BS 10008:2008, which is withdrawn.

Information about this document

This is a full revision of the standard, and introduces the following principal changes:

- recognition of the significant changes in recent years of how information is managed as an asset in organizations;
- inclusion of structured data within the scope;
- inclusion of the importance of stewardship of electronic information as an organizational activity;
- restructured to enable alignment with the ISO Management System Standards structure as defined in the ISO/IEC Directives, Part 1, Annex SL [1].

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

Information is an organizational asset that needs to be managed throughout its lifecycle; it is frequently required to be used within and outside the organization for demonstrating compliance and/or dispute resolution. If the authenticity or integrity of the information cannot be trusted then conclusions based upon it could be discredited. This British Standard addresses how information needs to be managed by an organization, in an information management system, to enable it to have strong evidential weight and be demonstrably trustworthy with regard to its authenticity and integrity whenever during its lifecycle it is needed to be used – whether for business, compliance, legal or other dispute resolution purposes.

BSI has published a *Code of Practice for Evidential Weight and Legal Admissibility*, BIP 0008 [2], [3], [4] (formerly PD 0008) since 1996. This Code of Practice has been widely adopted and is referenced, for example, by the Lord Chancellor's *Code of Practice on the management of records* published under Section 46 of the Freedom of Information Act 2000 [5]. In Scotland this is the *Code of Practice on records management* issued under Section 61 of the Freedom of Information (Scotland) Act 2002 [6].

BIP 0008 consists of the following three parts, which have been revised to provide information and guidance for the implementation of various sections of this British Standard:

- 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. The compliance workbook, BIP 0009 [7], provides a tool that enables the demonstration of compliance with this British Standard along with the appropriate parts of BIP 0008.

If an organization's electronic information management system conforms to this British Standard, it is anticipated that the evidential weight of electronic information managed by the organization 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 revision of this British Standard has been structured along the lines of the standardized structure of ISO Management System Standards, as defined in ISO/IEC Directives, Part 1, Annex SL [1] such that its implementation can be aligned and synchronized with other management system standards, such as the following:

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

- BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*;
- BS EN ISO 14001, *Environmental management systems – Requirements with guidance for use*.

1 Scope

This British Standard specifies requirements for the implementation and operation of electronic information management systems, including the storage and transfer of information, with an objective of enabling the user to ensure the authenticity and integrity of the information is maintained, so that it is trustworthy and is either accepted without dispute or successfully resists challenge. These issues are important where the information might be used as evidence – whether for business, compliance, legal or other dispute resolution purposes.

This British Standard covers:

- a) the management of the availability of electronic information over time;
- b) the electronic transfer or communication of electronic information;
- c) the linking of electronic identity to particular electronic information, including the use of electronic signatures and electronic copyright systems, as well as the verification of electronic identity.

This British Standard also includes requirements for the stewardship and accountability of the management of information throughout its life cycle.

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

This British Standard applies to electronic information in any form, including general office documents, electronic images and information held in databases and other electronic systems. The information may be alphanumeric, image based and/or voice/video recordings.

This British Standard does not cover processes used to evaluate the authenticity of information prior to it being captured or created in the system.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 big data

data that cannot be processed using conventional database management tools or data processing applications due to its size

NOTE There is currently no internationally recognized standard definition of the term "big data".

3.2 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

[SOURCE: NIST Special Publication 800-145 [8]].

NOTE BIP 0117:2010 [9] addresses this area.

3.3 compound document

information constructed from a number of separate digital documents

3.4 conversion

translation of electronic information from one file format to another

3.5 document

information stored on media

[SOURCE: BIP 0008]

3.6 electronic image

electronic representation that depicts or records a visual perception

NOTE 1 This electronic representation could be in two dimensions (e.g. document, picture, map) or three dimensions (e.g. CAD model, hologram, sculpture).

NOTE 2 This electronic representation could be in a raster (e.g. bit-map) or vector format.

3.7 information management

processing and/or storage of information in a controlled manner

3.8 lossy compression

type of information which results in the de-compressed information having less detail than the originating information before compression

3.9 management system

set of interrelated or interacting elements of an organization to establish policies (3.15) and objectives and processes (3.17) to achieve those objectives

NOTE 1 A management system can address a single discipline or several disciplines.

NOTE 2 The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

NOTE 3 The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

[SOURCE: ISO/IEC Directives, Part 1, Annex SL [1]]

3.10 media

material upon which information is recorded

[SOURCE: BS ISO 18913]

3.11 metadata

data about data

[SOURCE: BIP 0008]

3.12 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.

3.13 nonconformity

non-fulfilment of a requirement

[SOURCE: BS EN ISO 9000; BS EN ISO 14001]

3.14 organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

NOTE The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: BS ISO/IEC 27000:2014]

3.15 policy

intentions and direction of an organization as formally expressed by its top management

[SOURCE: ISO/IEC Directives, Part 1, Annex SL [1]]

3.16 procedure

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

3.17 process

set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: ISO/IEC Directives, Part 1, Annex SL [1]]

3.18 record

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

[SOURCE: BS ISO 30300:2011]

3.19 stewardship

responsibility for information assets used by the organization

[SOURCE: based on BS ISO 20121]

3.20 system

set of interdependent elements constituted to achieve a given objective by performing a specified function

[SOURCE: BS ISO 14620-2]

3.21 top management

person or group of people who directs and controls an organization at the highest level

NOTE Top management has the power to delegate authority and provide resources within the organization.

3.22 transfer

movement of electronic information from one system to another

3.23 workers

individuals working under the control of an organization, including employees, temporary staff, contractors and consultants

4 Context of the organization

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

4.1 General

The organization's top management shall determine:

- a) the external and internal issues that are relevant to information authenticity and integrity (see 4.2);
- b) the requirements of internal and external parties that are relevant to information authenticity and integrity (see 4.3);
- c) the boundaries and applicability of the information management system with respect to authenticity and integrity (see 4.4).

4.2 Issues

A risk management process shall be used to identify issues.

NOTE The risk management processes defined in BS ISO 31000 may be appropriate.

4.3 Requirements

When determining information management requirements, legal and regulatory requirements, duty of care, contractual obligations and information stewardship throughout the information lifecycle shall be included.

4.4 Boundaries and applicability

When determining the scope of the information management system, issues (4.2) and requirements (4.3) shall be taken into consideration. Where only part of the information held by the organization is included (for example, a single department or a single process could be defined as the scope of the system), the scope of the system shall be documented as part of the policy statement (see 5.2.2 and 5.2.3).

5 Leadership

Objective: To provide leadership in the management of electronic information and ensure that the appropriate resources are allocated to the various tasks.

5.1 Leadership and commitment

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

NOTE 1 The top management team might consist of a Board of Directors, a Chief Executive and his/her top staff, the partners or an owner of a sole trader company.

The policy shall address the whole lifecycle of the information and shall identify the role of the information steward(s), responsible for the information at each stage of its lifecycle.

NOTE 2 The information stewardship may be transferred between individuals at different stages in the lifecycle of an information asset. This continuity of stewardship is important to demonstrate an unbroken chain of management and accountability throughout the information life.

The policy shall cover:

- a) the storage of electronic information (see 5.2.2);
- b) the transfer of electronic information between systems (see 5.2.3).

The policy shall be linked to or combined with the organization's information security policy (see 5.2.4).

NOTE 3 In some organizations this might be called an information risk management policy.

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

The policy shall have a custodian, responsible for its maintenance and review in accordance with the organization's approved review procedure.

The policy shall be integrated into the organization's processes.

Sufficient resource shall be available to implement the policy and to ensure the relevant outcomes are achieved and, where appropriate, improved.

5.2 Policy statements

5.2.1 General

NOTE This subclause gives details of the required policy statements covering the storage and transfer of electronic information.

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

5.2.2 Electronic storage policy statement

The electronic storage policy statement 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 as a minimum 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) the compliance with applicable legislation and/or regulation;
- e) any consultations that the organization needs to undertake (see 5.4);
- f) the definition and allocation of roles and responsibilities for information stewardship and storage (see 5.3);
- g) the use of the appropriate electronic storage technology (see 8.6.1);
- h) the use of the appropriate electronic file formats (see 8.6.3);
- i) the use of compression technology (see 8.6.5);
- j) the use of encryption technology (see 8.12.3);
- k) the management of the linking of electronic identity to information (see 8.10);
- l) the retention and disposal of information, including the management of legal holds (see 8.11);
- m) the auditing of the information management system (see 9.2).

NOTE Other elements may be included.

5.2.3 Electronic transfer policy statement

The electronic transfer policy statement 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 as a minimum 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 5.3);
- c) the communication of specific types of information (see 8.7);
- d) the use of data compression (see 8.6.5);
- e) the use of particular systems for the transfer of electronic information (see 8.7);
- f) the receiving of transferred electronic information (see 8.7);
- g) the management of the linking of electronic identity to information (see 8.10);
- h) the use of encryption (see 8.12.3);
- i) the auditing of the information communication system (see 9.2).

NOTE Other elements may be included.

5.2.4 Information security policy

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

5.2.4.1 General

The organization shall ensure that the information management and transfer systems operate within the organization's information security policy.

The information security policy shall cover:

- a) the storage of electronic information over time (see 5.2.4.2);
- b) the transfer of electronic information between systems (see 5.2.4.3).

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.

5.2.4.2 Storage security policy statement

Where electronic storage of information over time is undertaken, the storage security policy statement 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 5.3);
- 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 8.12.2);
- 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.

5.2.4.3 Transfer security policy statement

Where electronic transfer of information is undertaken, the transfer security policy statement 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 5.3);
- 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 8.10);
- 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.

5.3 Roles and responsibilities of workers

5.3.1 General

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

5.3.2 Top management

Top 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 manage the information management system (see 5.3.3);

- c) appoint one or more persons, who, irrespective of other responsibilities, shall be responsible and accountable for the stewardship (see 5.3.4) throughout the information lifecycle of each information asset managed within the information management system.

NOTE For smaller organizations, responsibility for the information management system may be taken by a single identified individual as part of a wider job portfolio.

5.3.3 Individual or team responsible for managing the system

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

- a) follow a systematic and organized approach to monitoring known system conformity issues and recommending appropriate action;
- b) be business-focused and aware of the current state of the business and its priorities;
- c) be able to communicate at all levels within the organization;
- d) have a good understanding of the risks involved should the authenticity, integrity and/or availability of the information be compromised.

5.3.4 Information stewards

Information stewards, who are responsible and accountable for specific information assets, shall:

- a) follow a systematic and organized approach to monitoring information authenticity, integrity and quality conformity issues and recommending appropriate action;
- b) be business-focused and aware of the current state of the business and its priorities;
- c) be able to communicate at all levels within the organization;
- d) have a good understanding of the risks involved should the authenticity, integrity and/or availability of the specific information assets be compromised.

5.3.5 All information users

All information users shall:

- a) capture or use information at the proper time and using the proper information systems and processes;
- b) ensure the accuracy and completeness of information they create or use;
- c) report inaccuracies or inconsistencies of information and/or processes or systems that capture, report, consolidate or manage that information.

NOTE 1 There should be a reciprocal responsibility on the person the report described under c) is made to for action taken and results to be communicated back to the report originator.

NOTE 2 Attention is drawn to the responsibilities of users for the management of information that is subject to the Data Protection Act [10] and the Freedom of Information Act [5]; additional user responsibilities may be added to those above which are particularly pertinent to information authenticity and integrity.

5.4 Legal and regulatory environment

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

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

6 Planning

Objective: To ensure the appropriate security measures (based on risk assessments) that address the maintenance of information authenticity and integrity are identified and implemented.

6.1 Actions to address risks and opportunities

6.1.1 General

When planning an information management system, the issues and requirements identified in 4.2 and 4.3 shall be taken into account by determining the risks and opportunities that need to be addressed in order to:

- a) ensure the intended outcomes can be achieved;
- b) prevent and/or reduce undesirable effects; and
- c) achieve continual improvement.

6.1.2 Risk assessment

Objective: To identify and document the risks associated with authenticity, integrity and availability of information in the information management system.

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

Where available, the risk assessment process shall be that normally used by the organization. It shall include:

- a) the establishment and maintenance of risk criteria;
- b) the identification of risks and risk owners;
- c) the analysis of risks; and
- d) the prioritization of risks for risk treatment.

NOTE 1 Compliance with BS ISO/IEC 27005 should be considered when identifying, evaluating, treating and managing information security risks.

NOTE 2 The impact of information authenticity or integrity that is used in dispute resolution being discredited normally exceeds the impact of authenticity or integrity compromise of other information, often by several orders of magnitude.

6.1.3 Risk treatment

A process for risk treatment shall be defined and applied to the risks identified in 6.1.2.

6.2 Objectives and achievements

The organization shall establish and document information management objectives with regards to authenticity and integrity which are:

- a) consistent with the policies;
- b) measurable (where practical);
- c) taking into account the risk assessment and risk treatment plans;

- d) monitored and communicated;
- e) updated as appropriate.

7 Support

Objective: To ensure that the appropriate resources and competences are allocated to the management of electronic information.

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information management system with regards to the authenticity and integrity of the managed electronic information.

7.2 Competence

The organization shall:

- 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 and/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 may include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

- a) the information management and transfer policies;
- b) their contribution to the effectiveness of the information management and transfer systems, including the benefits of trustworthy information authenticity and integrity; and
- c) the implications of not conforming with the information management and transfer systems requirements when information is used within or outside the organization.

7.4 Reporting and communication

The organization shall determine the need for internal and external communications relevant to the availability, authenticity and integrity of information within the information management and transfer systems including:

- a) what to communicate;
- b) when to communicate;
- c) with whom to communicate;
- d) who shall communicate; and
- e) the processes by which communication shall be effected.

A communication plan shall be established which identifies:

- 1) mechanisms for disseminating decisions;

- 2) mechanisms for collecting feedback;
- 3) mechanisms for the regular updating of risk information;
- 4) procedures for dealing with challenges to the authenticity and/or integrity of information being used as evidence;
- 5) procedures for ensuring that information that might be required as evidence is not subject to disposition in accordance with the organization's disposal schedule;
- 6) key individuals within the organization responsible for managing such communications;
- 7) mechanisms for determining or verifying the effectiveness of the communications.

7.5 Documented information

Objective 1: 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.

Objective 2: To enable the demonstration that the information management and transfer systems are operating in accordance with policy and procedures.

7.5.1 General

The organization shall have documentation covering the following aspects of the information management and transfer systems:

- a) the information management and information security policies (see 5.2.2 to 5.2.4);
- b) risk assessment (see 6.1.2);
- c) the roles and responsibilities and stewardship of workers (see 5.3);
- d) reporting and communications (see 7.4);
- e) system procedures (see 7.5.2.1);
- f) the key technology components (see 7.5.2.2);
- g) all activities carried out in relation to the information management system in the form of audit trails (see 7.5.3);
- h) internal audit reporting (see 9.2);
- i) management review (see 9.3);
- j) nonconformity and corrective actions (see 10.1);
- k) continual improvement (see 10.2).

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

Procedures shall be established to identify the controls over documentation.

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

7.5.2 Procedural documentation

7.5.2.1 Procedures manual

A manual shall be produced, detailing the procedures to be followed relating to the information management and transfer systems.

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 organization's retention policy.

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

7.5.2.2 System description

A description of the key technology components used for the electronic information management and transfer systems 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 organization's retention policy.

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

7.5.3 Audit trails

7.5.3.1 General

Audit trails shall be created, containing information which enables the sequence and details of activities related to the information management and transfer systems 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 8.6.2 and 8.6.4), e.g. system logs.

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.

7.5.3.2 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.

7.5.3.3 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.

7.5.3.4 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.

8 Operation

NOTE This clause gives details of essential operational procedures and states where controls should be in place. Additional controls should be added if required by the stated scope of compliance.

8.1 Information capture

Objective: To ensure that all electronic information is captured without significant loss.

8.1.1 General

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

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.

8.1.2 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 organization.

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 appropriate associated metadata is imported in conjunction with the imported digital object.

8.1.3 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 the scanned image is authentic and that any potential information loss due to the scanning processes is within formally agreed 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 8.1.2).

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 should be used as a test of scanner quality. The procedures specified in BS ISO 12653 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 organization'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 and consideration shall be given to the retention of the original information.

NOTE 3 The relevant quality issue might need to be recorded.

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 might 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.

8.1.4 Data extraction

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

8.1.5 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.

8.2 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.

8.3 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.

8.4 Information in structured databases

8.4.1 General

Objective: To ensure that information stored in structured databases can be demonstrated as authentic and reliable.

Where information is created, updated or stored in a structured database, policies, processes and procedures shall be implemented that enable the organization to demonstrate its integrity and authenticity.

Where information is created or updated in a structured database, procedures shall be implemented that enable the organization to demonstrate how its accuracy and authenticity can be confirmed and validated.

8.4.2 Big Data considerations

Objective: To ensure that information used in “Big Data” systems can be demonstrated as authentic and reliable.

The value of the “Big Data” that is held by the organization shall be assessed. Decisions based on the analysis of “Big Data” shall take into account any risks associated with the inability to demonstrate the authenticity and integrity of the “Big Data”.

Information classed as “Big Data” shall not be retained for longer than is necessary.

8.5 Version control

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

Where stored information can be amended or updated, 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.

8.6 Storage systems

8.6.1 Storage technology

Storage technology shall be chosen in accordance with the information management policy (see 5.2.2).

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

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

8.6.2 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 [8.6.4], 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 organization's requirements.

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

8.6.3 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 8.6.4). 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-1).

8.6.4 Conversion

Where replacement software (e.g. an operating system, database schema 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.

8.6.5 Compression

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

Where information is compressed during the storage or transfer processes, any changes to the information that might result in a loss of detail shall be evaluated, documented, validated and approved as not impacting authenticity or integrity.

Where lossy compression techniques are used, the procedures and processes shall be in accordance with the storage and/or transfer policy and, prior to the policy being established, the effect of the information loss at the compression settings to be employed shall be evaluated, accepted by the organization and the evaluation and acceptance processes formally recorded.

8.7 Information transfer

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

8.7.1 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.

8.7.2 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.

8.7.3 Message transmission systems

Where message transmission systems are used (e.g. email, SMS messages, social media), 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 names or pseudonyms;
- e) use of passwords, digital signatures and other content management tools;
- f) use of "copy-to" and "blind copy-to";
- g) detection and elimination of malicious software;
- h) inclusion of attachments and embedded links;
- i) use for legal purposes such as contracts;
- j) avoidance of breach of copyright;
- k) accuracy in content and addressing where electronic business is conducted;
- l) management of and response to messages on receipt.

8.8 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. The use of search tools in conjunction with indexes might reduce indexing metadata generation overheads.

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 BS ISO 23081-2.

8.9 Authenticated output procedures

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.

8.10 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 significant, procedures which authenticate the identity of the person, organization 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 proofs used to associate physical to electronic identity are approved by the organization;

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

8.11 Information retention and disposition

Objective 1: To ensure that information stored in an electronic form is retained and disposed of in accordance with the organization's retention and disposal schedule.

Objective 2: 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.

8.11.1 Retention

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

Information shall be retained for no longer than the period as defined in the organization's retention schedule unless:

- a) the information is required to support existing and/or anticipated litigation;
- b) there is an external reason for longer retention.

8.11.2 Disposition

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

Information disposal procedures shall be established that are in accordance with the organization's information management and security policies (see 5.2).

Information shall be disposed of at the end of its retention period, in accordance with the organization's disposal policy (see 5.2.2). Disposal procedures shall ensure that all copies (including personal copies and backup copies) of documents being disposed of are identified and included in the relevant procedures.

Disposal of information in accordance with the schedules shall be suspended where the information might be required as evidence. Information that might be required as evidence shall not be disposed of, even if its end of retention period is reached.

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.

8.12 Information security procedures

Objective 1: To ensure that the information management system is operated in accordance with the information security policy.

Objective 2: To ensure that electronic information is protected from accidental or deliberate loss or modification during storage and/or transfer.

8.12.1 General

The organization shall establish procedures for ensuring that the information management system is operated in accordance with the information security policy (see 5.2.4).

8.12.2 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 to information or to the information management and transfer systems 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.

8.12.3 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.

8.12.4 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.

8.12.5 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 organization's back-up 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.

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

Retention of back-up information shall not compromise the effective, timely disposal of information that is to be duly disposed of in accordance with the retention and disposal procedures (see 8.11).

8.12.6 Business continuity planning

The organization 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 EN ISO 22301 gives details of business continuity management systems.

8.13 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.

8.14 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 organization'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 organization; they cannot be transferred to the responsibility of the external service provider.

8.14.1 Procedures

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

8.14.2 Compliance

Where a service provider claims compliance with this British Standard, the organization shall require that proof of compliance be demonstrated on request and at regular intervals through the appropriate access to policies, procedures, processes, documentation and audit trail information.

NOTE This might involve the provision of the relevant documentation and either a copy of the audit trail or the provision of access to the audit trail.

8.14.3 Security in transfer

The organization shall specify the security requirements for information whilst in transit between the organization 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.

8.14.4 Overseas

Where overseas service provision is used, the organization shall specify that all applicable legislative and, where applicable, regulatory requirements relating to the management of information are to be met.

8.15 Information management testing

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

The organization shall test its information management system to ensure that it meets business requirements for information availability, authenticity and integrity.

The organization shall:

- a) develop tests that are consistent with the scope of the information management system;
- b) have a programme approved by top 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 assesses the achievement of the aims and objectives of the test;
- g) produce a written report of the test, outcome and feedback, including required actions.

9 Performance evaluation

Objective: To monitor the performance of the information management system, using internal audit and management review procedures.

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the performance and effectiveness of the information management system.

The organization shall determine:

- a) what needs to be monitored and measured, including information management processes and controls;
- b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE The methods selected should produce comparable and reproducible results to be considered valid.

- c) when the monitoring and measuring shall be performed;
- d) who shall monitor and measure;
- e) when the results from monitoring and measurement shall be analysed and evaluated; and
- f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9.2 Internal audit

9.2.1 Audit requirements

The organization shall conduct internal audits at planned intervals to provide information on whether the information management system conforms to:

- a) its own requirements for its information management system;
- b) the requirements of this British Standard;

and whether it is implemented and maintained in an effective and timely manner.

9.2.2 Audit objectives

The organization shall:

- a) plan, establish, implement and maintain an audit programme, including the frequency, methods, responsibilities, planning requirements and reporting;
- b) define the audit criteria and scope for each audit;
- c) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
- d) ensure that the results of the audits are reported to relevant management; and
- e) retain documented information as evidence of the audit programme(s) and the audit results.

The audit programme shall take into consideration the importance of the processes concerned and the results of previous audits.

9.3 Management review

Top management shall review the organization's information management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

- a) the status of actions from previous management reviews;
- b) changes in external and internal issues that are relevant to the information management system;
- c) feedback on the information security performance, including trends in:
 - 1) nonconformities and corrective actions;
 - 2) monitoring and measurement results;
 - 3) audit results; and
 - 4) fulfilment of information security objectives;
- d) feedback from stakeholders;
- e) results of risk assessment and status of risk treatment plan; and
- f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information management system.

The organization shall retain documented information as evidence of the results of management reviews.

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.

10 Improvement

Objective: To maintain and improve the effectiveness and efficiency of the information management system, by the identification and correction of nonconformities.

10.1 Nonconformity and corrective actions

When a nonconformity occurs, the organization shall:

- a) react to the nonconformity, and as applicable:
 - 1) take action to control and correct it; and
 - 2) deal with the consequences;
- b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
 - 1) reviewing the nonconformity;
 - 2) determining the causes of the nonconformity; and
 - 3) determining if similar nonconformities exist, or could potentially occur;
- c) implement any action needed;
- d) review the effectiveness of any corrective action taken; and
- e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

- a) the nature of the nonconformities and any subsequent actions taken; and
- b) the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information management system.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN ISO 9000, *Quality management systems – Fundamentals and vocabulary*

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

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

BS EN ISO 22301, *Societal security – Business continuity management systems – Requirements*

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 14620-2, *Space systems – Safety requirements – Part 2: Launch site operations*

BS ISO 18913, *Imaging materials – Permanence – Vocabulary*

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

BS ISO 20121, *Event sustainability management systems – Requirements with guidance for use*

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

BS ISO 23081-2, *Information and documentation – Managing metadata for records – Part 2: Conceptual and implementation issues*

BS ISO 30300:2011, *Information and documentation – Management systems for records – Fundamentals and vocabulary*

BS ISO 31000:2009, *Risk management – Principles and guidelines*

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

BS ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

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*

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

Other publications

- [1] ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2013, Annex SL
http://www.iso.org/ISO/home/standards_development/resources-for-technical-work/ISO_IEC_directives_and_ISO_supplement.htm
(last accessed on 01 December 2014)
- [2] BRITISH STANDARDS INSTITUTION. BIP 0008-1, *Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008*.

- [3] BRITISH STANDARDS INSTITUTION. BIP 0008-2, *Evidential weight and legal admissibility of information transferred electronically – Code of practice for the implementation of BS 10008*.
- [4] BRITISH STANDARDS INSTITUTION. BIP 0008-3, *Evidential weight and legal admissibility of linking electronic identity to documents – Code of practice for the implementation of BS 10008*.
- [5] GREAT BRITAIN. Lord Chancellor's *Code of Practice on the management of records*. Section 46 Freedom of Information Act 2000. London: HMSO.
- [6] GREAT BRITAIN. *Code of Practice on records management*. Section 61 Freedom of Information (Scotland) Act 2002. London: HMSO.
- [7] BRITISH STANDARDS INSTITUTION. BIP 0009, *Evidential weight and legal admissibility of electronic information – Compliance workbook for use with BS 10008*.
- [8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *The NIST Definition of Cloud Computing, NIST Special Publication 800-145*. U.S. Department of Commerce, 2011.
- [9] BRITISH STANDARDS INSTITUTION. BIP 0117:2010, *Cloud Computing – A practical introduction to the legal issues*.
- [10] GREAT BRITAIN. Data Protection Act 1998. London: HMSO.

Further reading

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

BS ISO 19005-2, *Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)*

BS ISO 19005-3, *Document management – Electronic document file format for long-term preservation – Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)*

BS ISO 30301, *Information and documentation – Management systems for records – Requirements*

BS ISO/IEC 20000-2, *Information technology – Service management – Part 2: Guidance on the application of service management systems*

PD ISO/TR 23081-3, *Information and documentation – Managing metadata for records – Part 3: Self-assessment method*

PAS 99, *Specification of common management system requirements as a framework for integration*

Evidential weight and legal admissibility of information stored electronically

Code of practice for the implementation of BS 10008

Fifth Edition



Peter Howes and Alan Shipman

First published 1996
Second edition 1999
Third edition 2004
Fourth edition 2008
Fifth edition 2014

by

BSI Standards Limited
389 Chiswick High Road
London W4 4AL

© The British Standards Institution 2014

All rights reserved. Except as permitted under the Copyright, Designs and Patents Act 1988, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior permission in writing from the publisher.

Whilst every care has been taken in developing and compiling this publication, BSI accepts no liability for any loss or damage caused, arising directly or indirectly in connection with reliance on its contents except to the extent that such liability may not be excluded in law.

While every effort has been made to trace all copyright holders, anyone claiming copyright should get in touch with the BSI at the above address.

BSI has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this book, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

The rights of Peter Howes and Alan Shipman to be identified as the authors of this Work have been asserted by them in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

Typeset in Great Britain by Letterpart Limited, www.letterpart.com

Printed in Great Britain by Berforts Group, www.berforts.co.uk

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 978 0 580 85676 1

Contents

Foreword	vii
Acknowledgements	viii
Introduction	1
General	5
1 Context of the organization	8
1.1 General	8
1.2 Issues	8
1.3 Requirements	8
1.4 Boundaries and applicability	9
2 Leadership	10
2.1 Leadership and commitment	10
2.2 Policy statements	10
2.3 Roles and responsibilities of workers	23
2.4 Legal and regulatory environment	23
3 Planning	24
3.1 Actions to address risks and opportunities	24
3.2 Objectives and achievements	25
4 Support	27
4.1 Resources	27
4.2 Competence	27
4.3 Awareness	27
4.4 Reporting and communications	27
4.5 Documented information	28
5 Operation	40
5.1 Management overview	40
5.2 Information capture	40
5.3 Self-modifying files	62
5.4 Compound documents	63
5.5 Information in structured databases	64
5.6 Big data considerations	68
5.7 Version control	70
5.8 Storage systems	73
5.9 Information retention and disposal	77
5.10 Information transfer	79
5.11 Indexing and other metadata	85
5.12 Output	87
5.13 Identity	88
5.14 Information security procedures	88
5.15 System maintenance	95
5.16 External service provision	96
5.17 Information management testing	102
6 Performance evaluation	103
6.1 Monitoring, measurement, analysis and evaluation	103
6.2 Internal audit	103
6.3 Management review	105

7 Improvement	108
7.1 General	108
7.2 Nonconformity and corrective actions	108
7.3 Continual improvement	109
Annex A Changes between the 2008 and 2014 versions	111
A.1 General	111
A.2 Editorial changes	111
A.3 Technical changes	112
Annex B Development history	113
Annex C Definitions	115
Annex D Example information management policy statement	124
Annex E Records management	128
Annex F Application of controls	129
Annex G References	134
Annex H Legal issues	138
H.1 Background	138
H.2 Information management and legal admissibility	138
H.3 Weight of evidence and document destruction	139
H.4 Authenticity	139
H.5 Originals and copies	140
H.6 Born digital environment	140
H.7 Digitized images	141
H.8 Photocopies, microfilm and electronic images	141
H.9 Information storage	142
H.10 Storage and access procedures	142
H.11 Retrieval/viewing software	143
H.12 United Kingdom legislation	143

Foreword

Evidential weight and legal admissibility of information stored electronically — Code of practice for the implementation of BS 10008 (referred to in this document as 'the Code') is primarily concerned with the authenticity, integrity and availability of electronically stored information, to the demonstrable levels of certainty required by an organization. It is particularly applicable where this stored information may be used as evidence in disputes inside and outside the legal system.

This is the fifth edition of the Code, which was first published by BSI in 1996. This edition is an editorial revision of the fourth edition (BIP 0008-1 (2008)). It is technically similar, with an extension of its scope to include information stored in databases and other electronic systems. It has also been restructured in recognition of the publication of BS 10008:2014, *Evidential weight and legal admissibility of electronic information — Specification* and can be considered to be a guide to the implementation of the British Standard in relation to information stored electronically.

Users of the previous editions should consider the advantages of assessing their information management systems in the light of this new edition, and amend their systems and/or documentation where appropriate. Guidance is given in Annex A of this part of the Code on the major differences between this version and the previous versions.

This publication is the first part of BIP 0008, which is made up of the following:

- BIP 0008-2 (2014), *Evidential weight and legal admissibility of information transferred electronically — Code of practice for the implementation of BS 10008*;
- BIP 0008-3 (2014), *Evidential weight and legal admissibility of linking electronic identity to information — Code of practice for the implementation of BS 10008*.

The Code is published by BSI in recognition of the large number of implementations of electronic information management systems, and of the continuing uncertainty about the legal acceptability of information stored on these systems. It provides good practice guidance for the electronic creation, storage and retrieval of information.

Acknowledgements

The Editors would especially like to thank the BSI Legal Admissibility Editorial Board and Panel and committees IDT/1, *Document management applications* and IDT/1/-/5, *Revisions of BS 10008* for their contribution to the current and previous editions of this publication, in particular for their business foresight and tireless reading of the manuscript. Their suggestions for improvements added value to the final publications.

The members of IDT/1 are Martin Bailey, Ian Curington, Aandi Inston, Marc Fresko, Peter Howes, Philip Jones, Andrew Kenny, Bill Mayon-White, Roger S Poole, Nick Pope, Ian Walden, Leonie Watson, Andrew Pibworth, Neil Pitman, Alan Shipman and Tom Wilson.

The members of IDT/1/-/5 are Elisabeth Belisle, Bernie Dyer, Peter Howes, Richard Jeffrey-Cook, Bill Mayon-White, Roger S Poole, Alan Shipman, Rod Stone and Tom Wilson

In particular, we would like to thank Jennifer Carruth from BSI for her excellent advice and copy-editing work on BS 10008:2014.

Peter Howes
Alan Shipman
(Editors)
Group 5 Training Limited

The Editors would also like to thank the following organizations for reviewing the previous editions of this publication:

Association of Chief Police Officers (ACPO);
Association for Payment Clearing Services (APACS);
British Computer Society (BCS) – Information Risk Management & Audit (IRMA) specialist group;
National Audit Office (NAO);
Police Information Technology Organisation (PITO);
The National Archives (TNA).

The first version of the Code, published in 1996, was authored by the following: Rob Allen, Bernard Dyer, Ian Galbraith, Bill Mayon-White, Roger Peggram, Alan Shipman (Editor) and Malcolm Smith.

The first version of the Code was sponsored by the leading information management users and trade organizations in the UK, namely: Computing Suppliers Federation, Information and Document Management Association, Legal Images Initiative consortium and UKAIIIM Standards Committee.

The first version of the Code was developed with the assistance of a group of leading UK companies, consultants and associations: Advent Imaging Limited, AMEC Construction, APACS, Ashford Borough Council, Association of Computer Telephone Integration Users and Suppliers (ACTIUS), Autotrol Technology Limited, Bell and Howell, Bird and Bird, Blueprint, Brighton University, British Computer Society Computer Audit Specialist Group (BCS-CASG), British Standards Institution (BSI/DISC), Centre for Commercial Law Studies (University of London), Cheque and Credit Clearing Company Limited, Cimtech Limited, Concordium Software Limited, Document Image Technology, European Commission, European Electronic Messaging Association (EEMA), Fujitsu Europe Limited, Group 5 Training Limited, Headway Technology Group, Hewlett-Packard Limited, Imtec Group, Intergraph (UK) Limited, Kodak, Lloyds TSB Group, Lombard Document Systems Limited, London Borough of Enfield, London Transport, Marc Fresko Consultancy, Maxoptix Europe Limited, Microgen (UK) Limited, MR Group plc, National Westminster Bank, North Hampshire Hospital, Oki Systems (UK) Limited, OMS Services Limited, Q Star Limited, Registration Board for Assessors, Royal Bank of Scotland, SBC Warburg, Scottish Nuclear Limited, SNS Systems Inc., Society of Archivists, Sony (UK) Limited, SSI Microcad, Staffware plc, Tekdata

Limited, Tower Technology, Trimco Enterprises Limited, UK Banks Credit Card Committee, Wicks and Wilson Limited, Workflow & Groupware Strategies, Workflow Management Coalition (WfMC), Xerox Imaging Systems and 3M (UK) plc.

BSI would also like to thank the following who reviewed the fifth edition of this book:

John Avallanet, Managing Director & Principal, Cerulean Associates LLC;
Diane Shillito, Quality Systems Manager, CDS;
Neil Maude, General Manager, Arena Group;
Elisabeth Belisle, Managing Director, Scandox.

Introduction

Management summary

It is essential that organizations are aware of the value of the information that they store, and that they execute their responsibilities under the 'duty of care' principle. This Code of Practice gives detailed guidance on the issues of information management, information security management and legal/regulatory requirements. The Code is arranged based on BS 10008, *Evidential weight and legal admissibility of electronic information — Specification*, and can thus be used as a guide to the implementation of this British standard.

Information security is significant when discussing legal admissibility issues. Where legal admissibility is being assessed, the main discussion is likely to be related to the authenticity of the stored information. When the electronic information was captured by the storage system, was the process secure? Was the correct information captured, and was it complete and accurate? During storage, was the information changed in any way, either accidentally or maliciously? When responding to these questions, information security implementation and monitoring will be significant evidence when asked to demonstrate authenticity.

Information as an asset

The board of directors (or other equivalent group) 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 a board of directors 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. But 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 has 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 has 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, should be properly identified, even if identification is not required for accounting purposes, for consideration as an asset of the business. On the other hand, the retention of information past its retention period can also be a business liability, for example an increased cost of storage.

Most organizations have extensive experience in the subjects and functions they address. Relatively few organizations have experience in the acquisition, processing, storage and transmission of information and fewer still in the responsibilities that arise when information is considered a business asset.

¹ In 1995, with the support of the KPMG IMPACT team, the Hawley Committee produced a report, *'Information as an Asset'*, with an objective of creating a set of guidelines for boards of directors on policies and procedures for managing information.

Purpose of the Code

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 the Code is to assist organizations in dealing with the implications, specifically concerning evidential and legal issues, of this technological evolution.

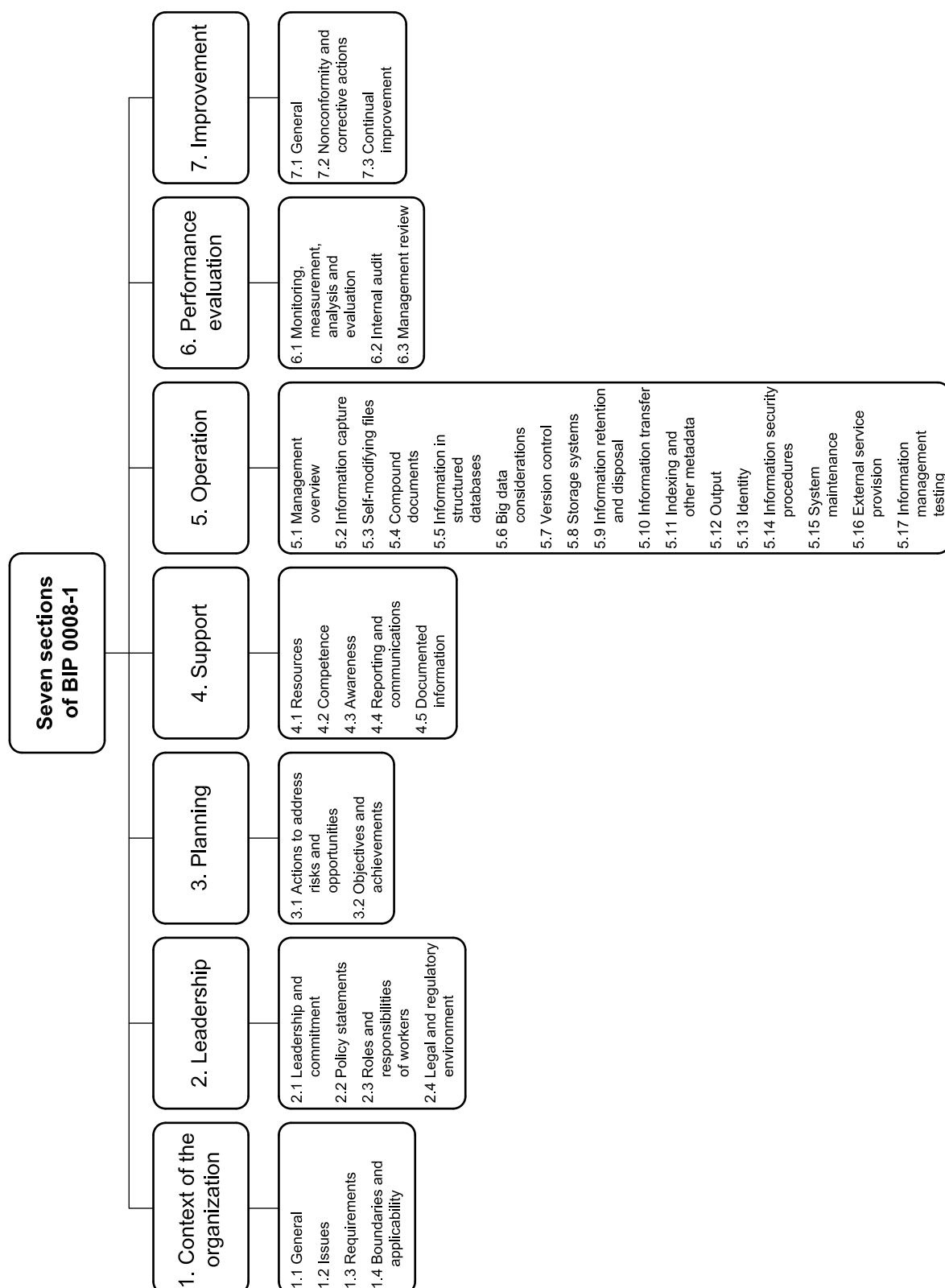
The Code provides a framework and guidelines, based on the provisions of BS 10008 that identify key areas of good practice for the implementation and operation of such electronic storage systems, whether or not any information held therein is ever required as evidence in the event of a dispute. As such, compliance with the Code (and therefore with BS 10008) should be regarded as a demonstration of responsible business management.

A more detailed explanation is provided in Annex B, to assist readers new to the subject or seeking background rationale for the guidance to good practice in the rest of the document.

Management framework

Chapters 1 to 7 of the Code 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 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements* where appropriate.

Previous versions of the Code were structured according to the four phases of the Plan-Do-Check-Act, or PDCA for short, which had been adopted by the majority of management systems standards. Recent changes to the structure of these management system standards (such as those for quality management (BS EN ISO 9001:2008, *Quality management systems — Requirements*), environmental management (BS EN ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*) and information security management (BS ISO/IEC 27001)) have taken place. The PDCA model emphasizes how critical it is for effective risk management that an ongoing management process is in place, and is exercised.



General

Scope

The Code describes the implementation and operation of information management systems that store information electronically and where the issues of authenticity, integrity and availability as required by legal admissibility and evidential weight are important.

DEFINITIONS (see also Annex C)

Authenticity – trustworthiness of origin and evidential content

Integrity – retention of the evidential content of the information

Availability – accessibility of the information as required

NOTE: Where the term 'system' is used in this document, it should be taken as meaning the 'information management system' that is being reviewed, unless otherwise stated.

The Code is for use with any information management system that stores information electronically, using any type of electronic storage medium including write-once-read-many (WORM) and rewritable technologies.

The Code is also for use with any type of database or other electronic system. Database files may potentially contain any type of data: for example, coded-character data, formatted text, images, computer-aided design (CAD) drawings, moving and still video images or voice data, or any combination of these. Database files may contain data of more than one type, and/or of more than one image. Database files may also include internally generated files, such as log files and audit trails.

Database files may be created by the information management system itself or by its users, or they may be imported into the system. The Code covers all such database files, whether created and/or imported directly or through a network, from the time at which the system assumes control of the database file.

The Code does not cover processes used to evaluate the authenticity of information 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.

The Code is also for use in the identification and development of policies and procedures as specified in BS 10008, in relation to the storage of electronic information. A companion to the British Standard and to the Code is the compliance workbook, BIP 0009 (2014), *Evidential weight and legal admissibility of electronic information — Compliance workbook for use with BS 10008*. This workbook enables a comprehensive assessment to be made of the user's information management system for compliance with the British standard. Completion of a copy of BIP 0009 for each system and associated storage and retrieval processes provides one means of satisfying key elements of the audit trail.

Voice, audio and video data

Data files may contain voice, audio and/or video information. Such files can be managed in accordance with the Code.

For all such files, once the recording is frozen, the file needs to be treated in the same way as any other data file as far as the Code 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 needs to have control of file integrity that is at least as good as that imposed by the Code for other types of information capture.

Where voice, audio and/or video data is stored, procedures for authentication of the source of the data need to be documented.

Applicability

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

Technology

It is important to utilize reliable and trustworthy technology to store electronic information 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 may 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).

The users

The Code is intended for:

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

Objectives

The objectives of the Code are to:

- improve reliability of, and confidence in, stored information;
- maximize the evidential weight that a court or other body may assign to presented information;
- provide confidence in inter-company trading;
- provide confidence to external inspectors (e.g. regulators and auditors) that the organization's information and business practices are robust and reliable.

The Code may be used as a common reference for business activities within and between organizations and for subcontracting or procurement of IT services or products.

Compliance

Each chapter of the Code contains a general description of the issues being addressed, followed by a list of 'key issues'. These key issues indicate the critical compliance points that need to be taken into consideration, and acted upon where appropriate, before compliance with the recommendations of the Code can be claimed. Compliance is claimed on a voluntary basis, by self-certification.

A compliance workbook (BIP 0009) has been published by BSI to enable an assessment of compliance with BS 10008 to be demonstrated. Where critical compliance points from the Code are not specifically included in the British standard, these points are included as an optional component in the compliance workbook.

Where compliance on a self-assessment basis is claimed, recommended compliance statements as shown in 6.3.4 should be used. See also 6.3 for further information on compliance audits.

It should be noted that, where compliance is assessed by a third party, liability for compliance will normally remain the responsibility of the organization.