Evidential weight and legal admissibility of information stored electronically

Evidential weight and legal admissibility of information stored electronically

Code of practice for the implementation of BS 10008

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

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

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 work in assisting with the drafting of the previous editions of this publication, for their business foresight, and for their tireless reading of the manuscript. Their suggestions for improvements added value to the final publications.

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 UKAIIM 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.

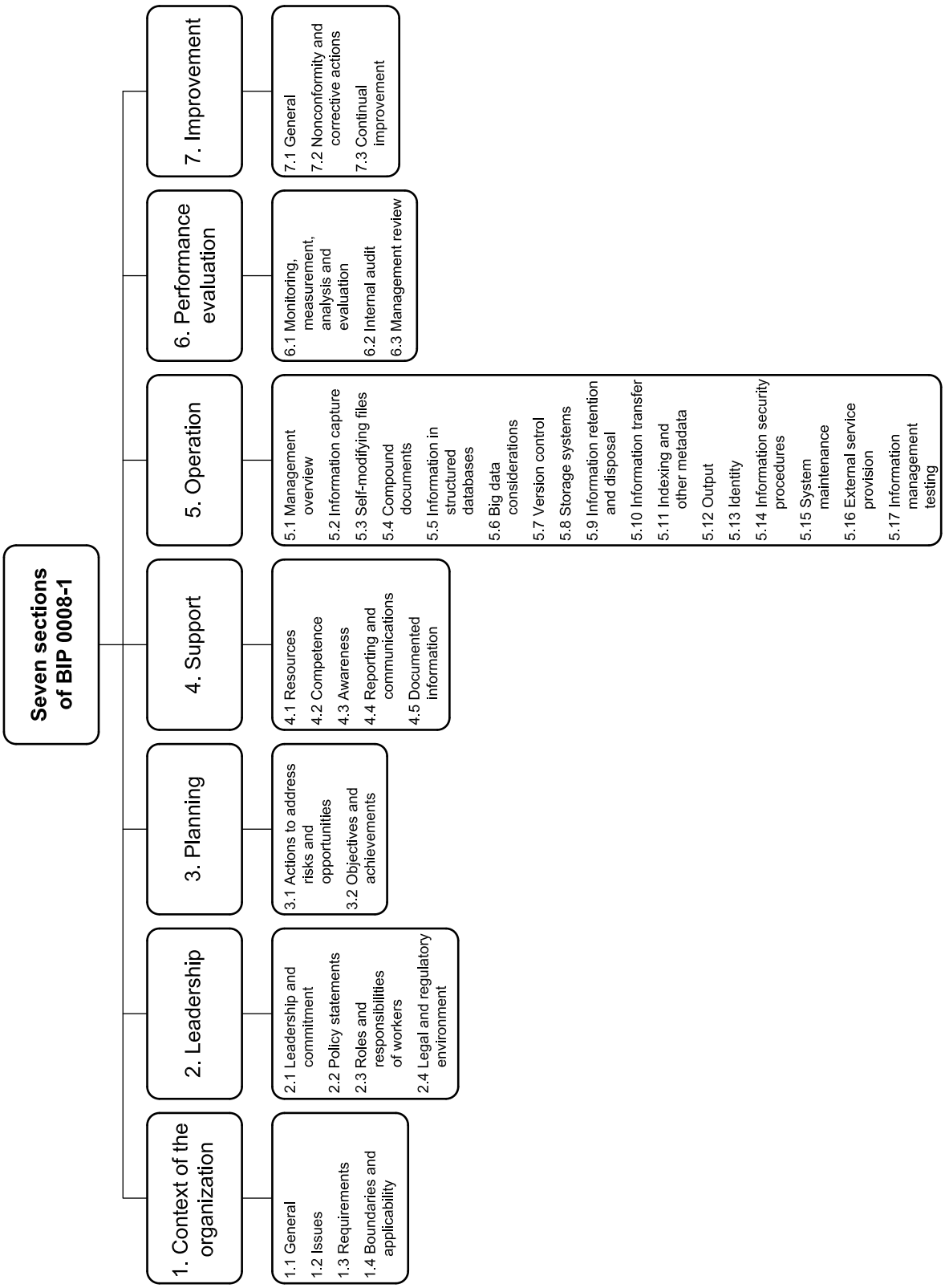
The Code provides a framework and guidelines, based on the provisions of BS 10008 that identify key areas of good practice for the implementation and operation of such electronic storage systems, whether or not any information held therein is ever required as evidence in the event of a dispute. As such, 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.

1 Context of the organization

1.1 General

This section of the Code relates to Clause 4 of BS 10008, 'Context of the organization'.

Everything an organization does involves using information in some way. The quantity of information can be vast, and there are many different ways of representing and storing it. The value of information used and the manner in which it is applied and moved within and between organizations may determine the success or failure of those organizations.

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

1.2 Issues

The organization needs to determine the external and internal issues that are relevant to its purpose and that may affect the authenticity and integrity of the information that it uses.

Typical issues that may be relevant include:

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

Policy statements as described in 2.2 should take into account those issues that are agreed to be relevant to the ability to demonstrate authenticity and integrity of information stored electronically.

When reviewing the relevant issues, a risk management process is the most appropriate to use when deciding upon actions to be undertaken. BS ISO 31000:2009, *Risk management — Principles and guidelines* provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using BS ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

1.3 Requirements

When establishing or reviewing the systems and/or processes that manage the evidential weight of information stored electronically, the organization needs to determine:

a) stakeholders that are relevant to the authenticity and integrity of information;
b) the requirements of these stakeholders relevant to that information;
c) the requirements for information stewardship within the organization.

NOTE: The requirements of stakeholders may include legal and regulatory requirements and contractual obligations.

Typical stakeholders may include:

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

The requirements of each stakeholder need to be taken into consideration when producing policy statements (see 2.2).

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

1.4 Boundaries and applicability

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

When determining this scope, the organization needs to consider:

a) the external and internal issues referred to in 1.2;
b) the requirements referred to in 1.3; and
c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope needs to be available as part of the policy document.

In many organizations, the authenticity and integrity of information will only be of importance to part of the overall information asset. As part of a project to implement BS 10008 and the Code, individual information assets need to be identified and a decision taken as to whether each should be included within the scope of the related policy statement.