Evidential weight and legal admissibility of information transferred electronically

Evidential weight and legal admissibility of information transferred electronically

Code of practice for the implementation of BS 10008

Peter Howes and Alan Shipman

bsi.

First published 1998
Second edition 2002
Third edition 2005
Fourth edition 2008
Fifth edition 2014

by

BSI Standards Limited
389 Chiswick High Road
London W4 4AL

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.

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 85677 8

Contents

Foreword

Evidential weight and legal admissibility of information transferred 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 transferred information, to the demonstrable levels of certainty required by an organization. It is particularly applicable where this transferred 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 in 1998 as PD 5000. This edition is an editorial revision of the fourth edition (BIP 0008-2 (2008)). It is technically similar, with an extension of its scope to include the transfer of 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 transferred 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.

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

- BIP 0008-1 (2014), *Evidential weight and legal admissibility of information stored 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 that has been transferred electronically. It provides good practice guidance for the trustworthy electronic transfer 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 edition of PD 5000, published in 1998, was sponsored by Group 5, in association with the Electronic Original Initiative.

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

Information transfer

Electronic information and documents that were created on electronic systems will frequently be sent under manual or automatic control to other electronic systems. Electronic transfer systems (see note) that send data (which itself is stored in compliance with BIP 0008-1) from one location to another need to be configured and operated in such a manner that the authenticity of the electronic information is not compromised. Many existing electronic information and document transfer systems are insecure, with the possibility of content being intercepted and amended during the transfer process without the knowledge of the sender or the recipient.

NOTE: In previous editions of this Code of Practice, the phrase 'electronic communications' was used. During the drafting of BS 10008, the term 'electronic transfer' was introduced. This update has been reflected in all three parts of BIP 0008 (2014). It should be noted that 'electronic transfer' includes all forms of electronic communications as discussed in earlier editions of the Code of Practice.

The Code seeks to define operational procedures that conform to 'good practice' in the field of electronic transfer. Following its recommendations ensures that the organization implements well controlled and structured systems, with minimum risk of authenticity being challenged, and with minimum risk of security breaches.

Compliance with the Code does not guarantee legal admissibility. It also does not follow that electronic information that is transferred by systems not in conformance to the Code is not legally admissible, but it may be more difficult to prove its integrity in court.

In some cases, where two parties reach prior agreement on a joint transfer policy, information and documents exchanged electronically within this agreement should be acceptable in court or other dispute resolution environments. In this case, legal advice needs to be sought on the wording of the agreement to ensure that the technical details are appropriate. Such agreements may not require conformance to the Code, but to do so would improve their acceptability to a court.

In order to provide widely applicable guidance, the Code does not specify system hardware or software configurations, and thus is technology independent.

Details of the content of transferred information are not relevant to the Code. Thus, the Code is equally applicable to simple 'message' documents, to complex multi-sectioned (compound) documents and information taken from and transferred to a structured database. In the Code, all such information is included under the term 'electronic transfers'.

Electronic mail (email), instant messaging (IM), web services, web forms, Extensible Markup Language (XML), mobile messaging (Short Message Service – SMS) and electronic data interchange (EDI) are increasingly being used for business communications. Many of these are 'free format' and give great flexibility of content. Chapter 1 gives guidelines for the development of an organizational policy for the creation, transmission and receipt of these unstructured forms of electronically transferred documents. Annex A gives further details of procedures that are applicable to unstructured messaging systems.

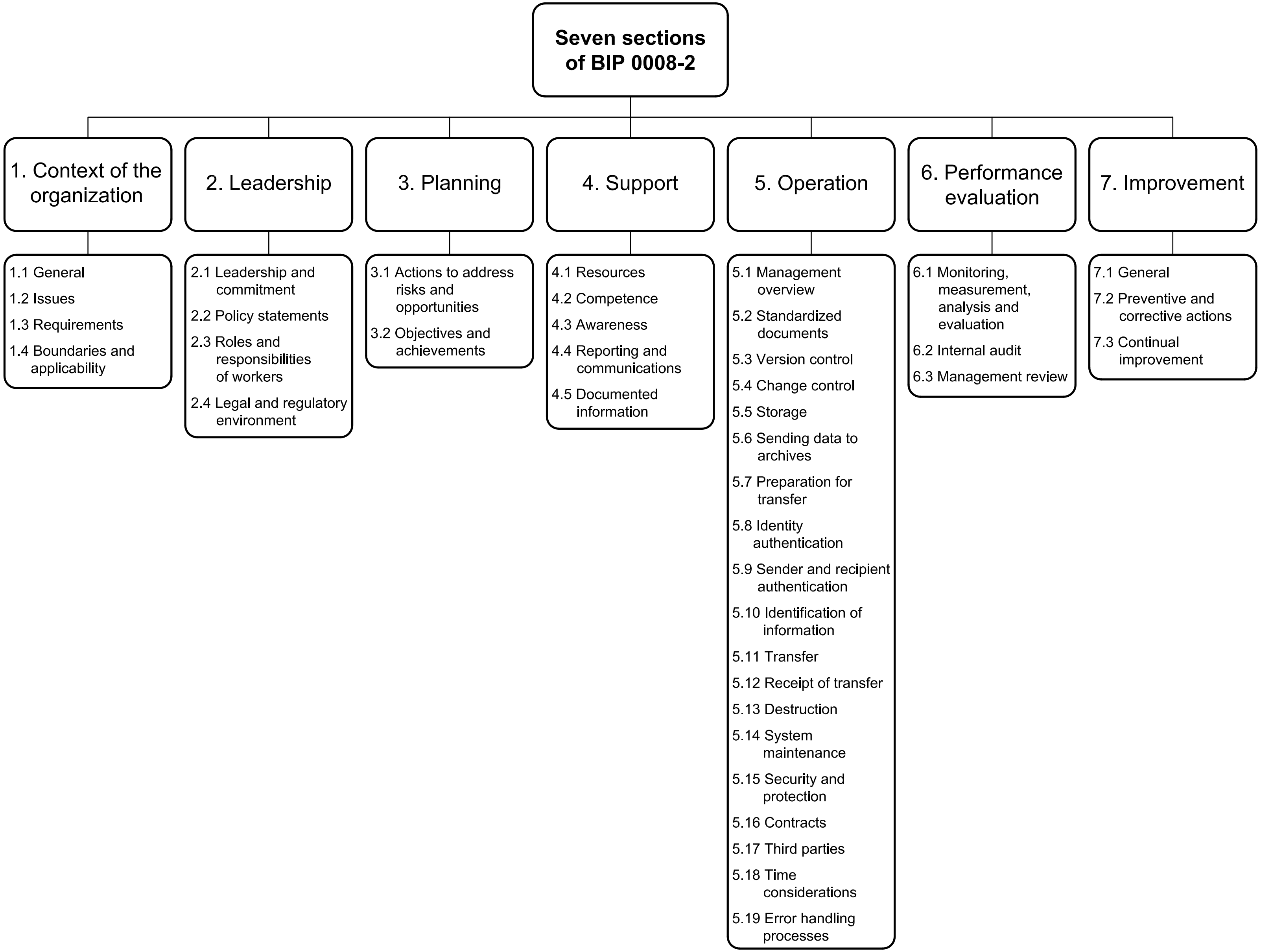
Purpose of the Code

Users of electronic transfer systems are being asked by their companies, government departments and other employers to review the legal issues relevant to their use. The application of these systems is changing the way in which many aspects of business and organizational life are operated, as electronic communications are increasingly replacing the more traditional paper-based methods. Different electronic transfer 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, which identify key areas of good practice for the implementation and operation of such electronic transfer systems, whether or not any such information 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.

Management framework

Chapters 4-7 of the Code are structured along the lines of the standardized structure of 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 system — Requirements* where appropriate.


Seven sections of BIP 0008-2
1. Context of the organization
1.1 General
1.2 Issues
1.3 Requirements
1.4 Boundaries and applicability
2. Leadership
2.1 Leadership and commitment
2.2 Policy statements
2.3 Roles and responsibilities of workers
2.4 Legal and regulatory environment
3. Planning
3.1 Actions to address risks and opportunities
3.2 Objectives and achievements
4. Support
4.1 Resources
4.2 Competence
4.3 Awareness
4.4 Reporting and communications
4.5 Documented information
5. Operation
5.1 Management overview
5.2 Standardized documents
5.3 Version control
5.4 Change control
5.5 Storage
5.6 Sending data to archives
5.7 Preparation for transfer
5.8 Identity authentication
5.9 Sender and recipient authentication
5.10 Identification of information
5.11 Transfer
5.12 Receipt of transfer
5.13 Destruction
5.14 System maintenance
5.15 Security and protection
5.16 Contracts
5.17 Third parties
5.18 Time considerations
5.19 Error handling processes
6. Performance evaluation
6.1 Monitoring, measurement, analysis and evaluation
6.2 Internal audit
6.3 Management review
7. Improvement
7.1 General
7.2 Preventive and corrective actions
7.3 Continual improvement

General

Scope

The Code describes procedures and processes for transferring electronic information from one computer system to another where the issues of authenticity, integrity and availability as required by the legal admissibility and evidential weight of the sent and/or received information is important, typically where two organizations are involved. Whilst specific systems are not addressed by the Code, the requirements of the system (both system and procedural) are included.

DEFINITIONS

Authenticity – trustworthiness of origin and evidential content

Integrity – retention of the evidential content of the information

Availability – accessibility of the information as required

Electronic document transfers are being used increasingly for electronic trading, where a 'document' is often described as a 'transaction' or a 'message' (e.g. in e-commerce applications). Such systems can be operated under the recommendations of the Code.

The sender and/or recipient of a data file may be a person, an organization, an application, an electronic system or a device. In many instances there will be a 1:1 relationship between the sender and the recipient; the Code applies to these and to situations where there are many recipients and a single sender.

The Code is for use with any type of computer file using a wide range of transfer infrastructures. Data files may contain binary data, text, images, computer-aided design (CAD) data, moving or still video images, audio or any combination of these or similar data types, or may be computer software files (or any combination of these).

Applicability

The Code is applicable to transfer systems that use computer networks or that use remote data file transmission systems via an electronic communications carrier. It also addresses circuit switched or electronic communications switched systems. The data file transmission may be by telephone circuit, cable, radio or satellite communications technology (or any combination of these).

As such it can be applied to message-based systems where a complete transaction is built up and sent as a whole to another user (e.g. fax, email, EDI using a value-added network (VAN), or e-business using the Internet). It may also be applied where a user is communicating interactively with a remote system and building up a transaction as a set of parts (e.g. web forms).

The users

The Code is intended for:

- end user organizations that wish to ensure that information transferred electronically may be used with confidence as evidence in any dispute, within or outside a court of law; and
- integrators and developers of information transfer systems that provide facilities to meet user requirements.

Objectives

The objectives of the Code are to:

- improve reliability of, and confidence in, transferred information;
- maximize the evidential weight that a court or other body may assign to presented information;
- provide confidence in inter-company trading; and
- provide confidence to external inspectors (for example, regulators and auditors) that the organization's information and business communications 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 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 (and with BS 10008) can be claimed. Compliance is claimed on a voluntary basis, by self-certification.

A compliance workbook (BIP 0009 (2014)) has been published to enable an assessment of compliance with BS 10008 to be completed. 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.

Typical compliance statements are shown in 6.3.4. See also 6.3 for further information on compliance audits.

Key requirements

Included in the controls for this part of the Code are a number of underlying criteria that, when complied with, provide assurances that electronic transfers have been sent and received in a controlled and understandable manner. As such they are applicable to both sender and recipient of the electronic transfer.

The transferred information should be stored in accordance with BIP 0008-1. The key requirements for maximizing the evidential weight of electronic messages are as stated in Table 1.

Sender authentication	Proving the sender identity (see BIP 0008-3)
Integrity	Ensuring the content of the electronic transfer is what it purports to be
Identification	Identifying the electronic transfer
Date and time of transfer	Identifying the time of transfer
Confirmation	Confirming receipt
Date and time of receipt	Identifying the time of delivery and/or collection
Recipient authentication	Proving the recipient identity (see BIP 0008-3)

Table 1 – Key requirements

Trusted third-party services

Many current electronic transfer systems may fail to provide adequate assurances concerning electronic transfer delivery. Delivery of an electronic transfer by a trusted third-party service provider can, in normal circumstances, provide strong independent evidence of the key recommendations detailed in 2.2.3.8. As such, use of these facilities can provide equal or greater evidential weight compared with that provided by an electronic transfer not using this facility.

EXAMPLE

Email has become an essential business tool, but it must be used with care if the sender or recipient is to rely upon email in the event of a dispute. It is not technically difficult to make an email appear to come from someone other than the real sender. This ID 'spoofing' is used extensively by spammers (see 5.7.3) to mask their identities. Even though the technologies used by internet email are powerful and interoperable, there is still no guarantee of immediate delivery, or in fact of delivery at any time. A sender simply requesting an email delivery receipt is not a totally reliable method for determining delivery as many systems are configured to withhold them; this is frequently to prevent spammers from using the delivery receipt request to validate email address details.

If you need to rely on sender identity or proof of delivery then additional safeguards need to be taken.

Where the trusted third-party service is retaining an archive copy of the message, this should be retained in accordance with BIP 0008-1.

Recipient's perspective

From the recipient's perspective, the main areas of challenge are:

- the sender is not who he or she purports to be;
- the electronic transfer was not received, or was received multiple times; and
- the information content of the electronic transfer has been changed in some way in transit.

EXAMPLE

An email may not be delivered at all, or it may be delivered multiple times. For many electronic transfers, repeated delivery is merely an inconvenience.

For many other electronic transactions, however, it is potentially dangerous:

- Would you really want to have duplicate payments appearing on your credit card statement?
- Does a business want to stop selling a particular product because it believes it is sold out, only to find that one of the apparent sales was, in fact, just a duplicate of a real order?

Such transactions need solid proof of delivery, so that a duplicate transfer is rejected and, if a receipt is not received within a predefined time, the message is re-sent.

Such proof of delivery is normally a fundamental component of the message queuing technologies that underpin web services and service-oriented architectures.

Electronic transfers transferred in compliance with the terms of the Code will allow the recipient to check sender authentication and electronic transfer identity and integrity.

Where a received electronic transfer is questionable, procedures that verify its origin and integrity need to be used. Such procedures may include sending the electronic transfer back to the supposed sender, with a request for a confirmation of receipt and integrity.

1 Context of the organization

1.1 General

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

Increasingly, electronic information is being sent from one electronic system to another, either within an organization or between organizations. The manner in which this movement of information occurs may determine the success or failure of the organization. Thus, transfer systems need to be secure, structured and auditable.

Electronic transfer systems need to be classified, structured and validated by the organization. Where information is received electronically from another organization, knowledge of the processes used to transfer the information is key to a successful, legally admissible electronic transfer system.

When defining a transfer policy, the relative importance of speed of delivery, both to the recipient organization and to the recipient in that organization, may be significant. Taking two extremes, direct transfer to a PC across the internet or via a carrier usually results in almost instantaneous transfer, whereas transfer by post may be measured in days.

BIP 0008-1 recommends the classification of all information used by an organization into ‘information types’. This classification leads to the creation of a ‘policy document’ which should be extended to accommodate the transferred information covered in this part of the Code.

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 transfers.

Typical issues that may be relevant include:

- the size and complexity of the organization;
- the level of business risk attached to being unable to demonstrate authenticity and integrity of transferred information;
- drivers for business efficiency improvements;
- specific stakeholder requirements; and
- 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, a 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 transferred electronically, the organization needs to determine:

- stakeholders that are relevant to the authenticity and integrity of information;
- the requirements of these stakeholders relevant to that information; and
- 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; and
- 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 (IAO’s) who will typically be those responsible for the processes that receive 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 transfers in order to establish its scope.

When determining this scope, the organization needs to consider:

- the external and internal issues referred to in 1.2;
- the requirements referred to in 1.3; and
- 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.