Evidential weight and legal admissibility of information transferred electronically

Code of practice for the implementation of BS 10008

Fifth Edition

Peter Howes and Alan Shipman

bsi.

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

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

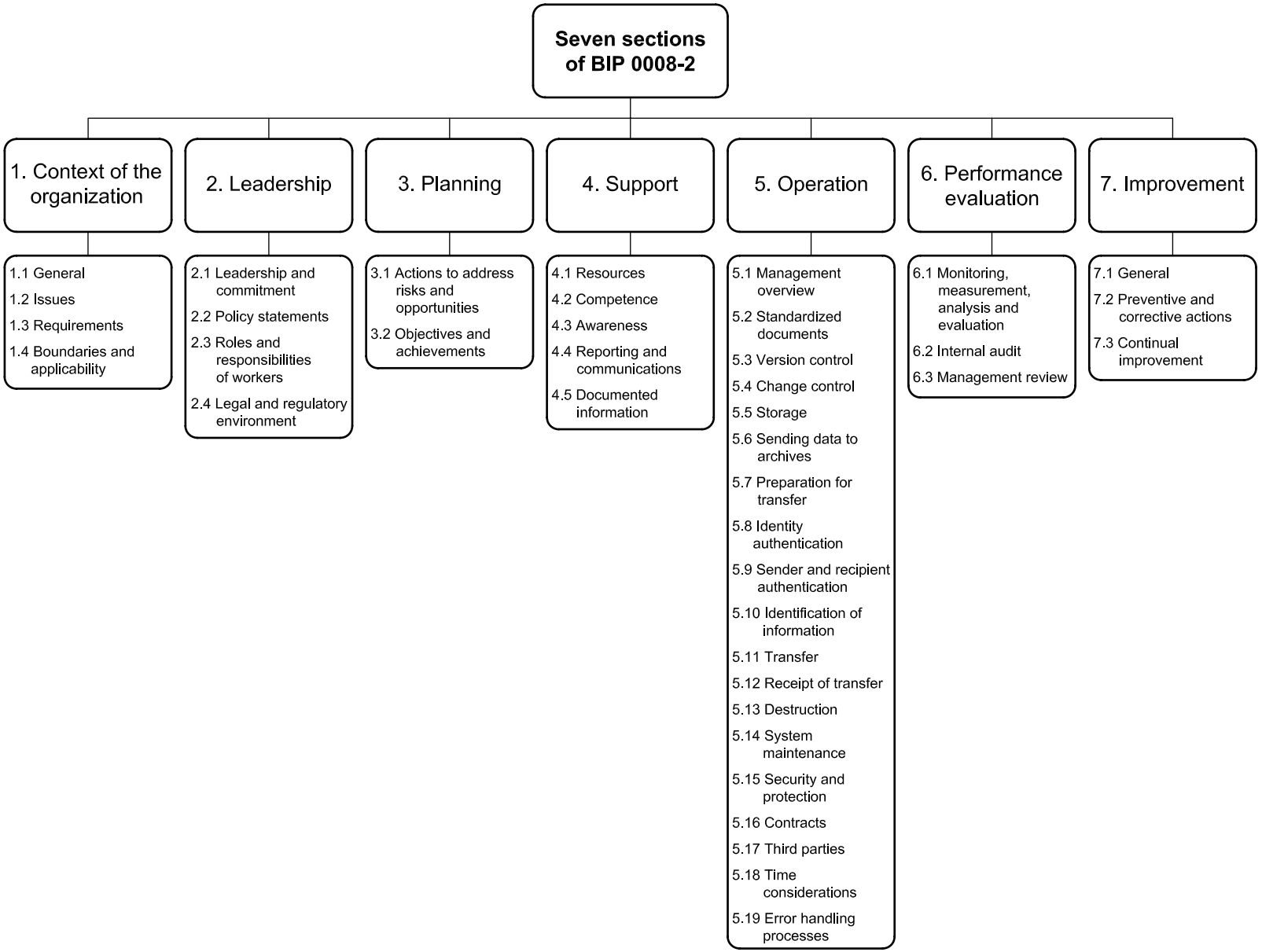
Users of electronic transfer systems are being asked by their companies, government departments and other employers to review the legal issues relevant to their use. The application of these systems is changing the way in which many aspects of business and organizational life are operated, as electronic 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.

2 Leadership

2.1 Leadership and commitment

This section of the Code relates to Clause 5 of BS 10008, 'Leadership'.

Top management needs to demonstrate leadership and commitment with respect to the management of the information authenticity and integrity by:

a) ensuring the information transfer policies and objectives are established and are compatible with the strategic direction of the organization;
b) ensuring the integration of the information transfer system requirements into the organization's processes;
c) ensuring that the resources needed for the information transfer system are available;
d) communicating the importance of effective information transfer and of conforming to the information transfer system requirements;
e) ensuring that the information transfer system achieves its intended outcome(s);
f) directing and supporting persons to contribute to the effectiveness of the information transfer system;
g) promoting continual improvement; and
h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

2.2 Policy statements

2.2.1 General

The British Standard specifies the contents of an electronic transfer policy statement, which covers the scope of the policy, requirements for procedures and technology and the responsibilities of the management of the systems. The British Standard also specifies the requirement for the top management team to set a clear policy direction and demonstrate support for, and commitment to, the management of the electronic information through the issue and maintenance of an information transfer policy.

The British Standard also specifies the contents of an information security policy within which the information transfer policy operates.

Policy documentation needs to be retained in compliance with the retention schedule.

KEY ISSUE

> Retain approved policy documents in line with the retention schedule.

2.2.2 Information transfer policy statement

2.2.2.1 Roles and responsibilities

The policy statement should include a statement, for each information type being transferred, of the party responsible for the information.

This party may be a person or a job function.

KEY ISSUES

> Identify individual responsibilities for information being transferred.

> Detail these in the policy statement.

2.2.2.2 Structure

Different types of information may be transferred within an organization, or between organizations, using different data file transmission systems. To enable implementation of such systems, the organization needs a policy statement that can be used to guide implementers, and to demonstrate to other parties that the systems used were in line with policy.

To implement the Code, the policy statement produced in compliance with BIP 0008-1 should be extended to include policy on electronic transfer.

The policy statement should be approved by the top management of the organization, and should be reviewed for relevance and content at regular intervals. The frequency for review should be appropriate to the application.

This period will typically be the same as the normal procedural audit cycle within the organization (e.g. annual or in the event of major changes to the system).

There will frequently be more than one type of data transmission system in use within an organization. The transfer requirements for each information type need to be reviewed, based on timeliness and service levels. Cost may also be a consideration.

In order to align transfer requirements with specific electronic information, an information 'type' designation should be allocated. These types may be described by application (e.g. financial reports or stock lists) or by information content (e.g. an invoice or an order).

Annex B includes an example electronic transfer policy statement, which may be used during the drafting of an organization's policy statement. It contains some 'typical' statements that may be appropriate in many policy statements.

The policy should set out guidelines for the appropriate transfer channel for each information type.

EXAMPLE

For some electronic transactions, multiple different transfer channels will be offered. These may have different characteristics, each variant of which needs to be considered.

For example, a single transaction could be sent by email, voice message, SMS or IM depending on sender or recipient preferences. Similarly, a website could offer a web form to complete or a downloadable form to be completed and emailed or faxed.

The policy statement should address, as a minimum, the requirements set out in Table 2. Other sections may be added where appropriate.

Topic	Content	Section of BIP 0008-2
Roles and responsibilities	Define responsibilities for information transfer	2.3
Transfers	Set guidelines for the transfer of specific electronic documents	2.2.2.3
Compression	Set guidelines for the use of data compression	2.2.2.4
Procedures	Set guidelines for procedures to be followed by workers when using transfer facilities to send electronic documents	2.2.2.5
Delivery/receipt	Set policy for procedures to be followed on delivery or receipt of a transferred file	2.2.2.6
Consultations	Consult with relevant bodies to ensure the legality of electronic transfer	2.2.2.7
Encryption	Set guidelines for the use of encryption	2.2.2.8

Table 2 — Information transfer policy statement

COMMENT – Transfer system requirements

A single message may have a different value to the sender and to the recipient. Transfer system requirements may thus vary depending upon individual requirements, or a combination of requirements.

EXAMPLE

Any electronic transaction involves two or more parties, and it is quite usual for its significance to be completely different for the different parties. It is, as a result, quite common for the controls and guidelines for a transaction (and its storage under the controls of BIP 0008-1) to be different for the different parties involved, even when they are within the same organization.

For example, an electronic expenses claim may involve an individual worker, his or her authorizing manager and the department responsible for payroll. The payroll department may have no first-hand knowledge of the worker or the manager and would, therefore, need independent evidence as to their identities, as linked to the claim (unlike the worker, who knows his or her manager). Both worker and manager are less concerned over authenticating the identity of the payroll department; they would realize that something was amiss when the expenses were not reimbursed with the pay.

KEY ISSUES

> Develop and have approved by top management an information transfer policy.

> Ensure it is reviewed at regular intervals, as appropriate to the application.

2.2.2.3 Transfers

There are many forms of technologies and procedures that can be used for electronic transfers. The organization's policy statement should set guidelines for the appropriate systems to be used for all corporate electronic transfers.

In particular, the use of structured and unstructured forms of electronic transfers should be included. Where unstructured electronic transfers are involved, corporate guidelines on message structures should be included within the policy statement, or referenced by it.

KEY ISSUE

> The policy statement should give guidance on the type of transfer technology to use in particular circumstances, and on the content and layout of unstructured transfers.

2.2.2.4 Compression

Some electronic transfers will need to be compressed before being transferred. This may be due to:

- a large file size (a smaller, compressed file will require less transmission time);
- a large number of individual files (these can be compressed into a single file); or
- the application of a compression key to improve electronic document security.

The policy statement should give guidance on when compression is to be used, and how to formulate compression keys.

See also BIP 0008-1 which gives further details of compression management.

KEY ISSUE

> The policy statement should give guidance on the use of compression tools.

2.2.2.5 Procedures

The policy statement should provide guidelines on the requirement for appropriate procedures to be followed when electronic transfers are being undertaken. Details of these procedures can be found in Chapter 5. These procedures may need to link to the organization's information security policy as detailed in 2.2.3.

KEY ISSUE

> The policy document should give guidelines on the procedures necessary to use the organization's electronic transfer systems.

2.2.2.6 Delivery/receipt

In relation to the Code, the critical procedural issues are related to the delivery of and the receipt of electronic transfers. Thus, the policy statement should give guidelines on how these procedures are to be developed, and to what standards. These procedures include:

- the avoidance of messages with illegal content;
- the avoidance of copyright issues;
- protection against malicious software;

- appropriate security procedures;
- the application of the organization's retention policies; and
- the avoidance of spam and similar messages (incoming and outgoing).

KEY ISSUE

> The policy statement should give guidelines on the procedures required to protect the organization, where electronic transfers are sent and/or received.

2.2.2.7 Consultations

There may be international, national and/or regional laws and/or regulations covering the transfer of information within, across, into or out of a country. It is thus essential to consult with relevant bodies to ensure the legality of transfer systems implemented.

In some countries, it is illegal to transfer particular types of electronic document. Organizational policies need to identify such documents and ensure that they are not transferred. Examples of such documents are those that contain obscenities or libellous statements or are encrypted to levels beyond those allowed.

The results of all consultations should be documented and retained in accordance with BIP 0008-1.

KEY ISSUES

> Relevant bodies should be consulted to ensure the legality of transfer systems implemented.

> The legality of transfer (including compression and encryption techniques) of particular types of electronic document should be determined, and any requirement adhered to.

2.2.2.8 Encryption

Encryption can be used to improve the security of electronic transfers, by the use of cryptographic techniques. Access to the unencrypted content of encrypted electronic information can be achieved by the application of the appropriate decryption algorithm and key.

The policy statement should state the organization's policy on when encryption is to be used, and how to formulate and manage encryption and decryption keys. It should also include policy on the security and access arrangements appropriate to encryption and decryption keys.

Typically, email messages may be encrypted at the organization's email gateway or at the sender's email client. The encryption can often be based on rules to enforce encryption to specified individuals and organizations or based on classification and content criteria. Care should be exercised when encrypted email is sent or received as to whether or not the message is in decrypted form within the organization; if it is not clear then this may render the message private to the sender and recipient rather than available as a discoverable asset to the organizations involved.

This message encryption should not be confused with encryption of the channel over which the email may traverse the network using SSL/TLS.

COMMENT – Encryption

Encryption of transfer messages may be to preserve confidentiality whilst in transit over the internet and/or within the sending (or receiving) organization.

If the internet is the concern, then encryption of email is an option worth considering. Messages are encrypted at an organizational level (e.g. mail server or mail relay) rather than at the level of the individual end user.

This will generally mean that there are fewer encryption keys to manage, but the message will be in an intelligible form within the organization.

KEY ISSUE

> The policy statement should give guidance on the use of encryption technology.

2.2.3 Information security management

2.2.3.1 Management overview

It is essential that an organization is aware of the value of the information that is transferred within the organization, or with its trading partners. This awareness includes an understanding of 'duty of care' principles.

The implications of an insecure electronic transfer system may be far reaching, and potentially damaging to an organization. In order to ensure the integrity of electronic information prior to, or after, transfer, it needs to be stored under the controls in BIP 0008-1. If, however, electronic information stored in compliance with BIP 0008-1 is transferred by a system not in conformance to the Code, its legal admissibility may be compromised.

Suitable guidelines, which specify system security requirements, may already exist in organizational policies or working practices. There may also be sector-specific guidance (e.g. financial or pharmaceutical), national or international standards, or legal requirements. Where these do not exist, suitable guidelines need to be developed, approved and implemented.

2.2.3.2 Information security principles

2.2.3.2.1 General

BS ISO/IEC 27002 is the UK reference document for information security management. Proof of compliance with the recommendations of this code of practice, when implemented within the boundaries covered by the Code, may provide helpful supporting evidence in court. It will indicate that the organization has exercised its duty of care, and it will assist the court in assessing the authenticity and integrity of the information.

BS ISO/IEC 27001 is an auditable specification for use in the certification of an information security management system against the standard.

Compliance with the recommendations of BS ISO/IEC 27002 or certification against BS ISO/IEC 27001 should not be regarded as an alternative to compliance with the recommendations of the Code.

BS ISO/IEC 27001 includes details of an information security model, classifying information security into three areas (the 'CIA' principle):

- Confidentiality;
- Integrity;
- Availability.

The relevance of all three of these principles should be reviewed and suitable procedures and processes implemented.

KEY ISSUE

> Information security standards provide auditable systems that enable organizations to demonstrate a duty of care in relation to stored information.

2.2.3.2.2 Confidentiality

Where appropriate, data being transferred should be protected from unauthorized access.

COMMENT – Information security

Confidentiality is about protecting data from unauthorized access. Formerly, information security used to primarily focus on confidentiality (rather than confidentiality, integrity and availability), ensuring that information is not available outside the intended authorized group. Whilst this is important and in some cases critical to the organization, it is not the most important security issue relevant to demonstration of strong evidential weight and consequently, this part of the Code.

KEY ISSUE

> Ensuring confidentiality in electronic transfers should be as appropriate to business needs. Confidentiality is not an important requirement of the Code.

2.2.3.2.3 Integrity and authenticity

Integrity is about ensuring that the content of a data file is unchanged; authenticity is about ensuring that it is what it purports to be.

Thus, both integrity and authenticity are key to the achievement of strong evidential weight and legal admissibility, ensuring data accuracy and completeness. When considering security, it is necessary to assess the risk of integrity or authenticity being compromised and to compare that with the cost of protection against such compromise. Security measures may include the application of encryption technology to reduce the risk of changes to information.

Procedures and processes should be implemented to ensure the integrity of electronic information during transfer. Some systems use file names linked to message authentication codes (MACs) or digital signatures for this purpose (see 5.7.8).

Data recovery procedures, to be implemented in the case of failure of the electronic information transfer system, should be such as to maintain the integrity of the relevant data.

KEY ISSUE

> Ensuring integrity and authenticity are the key issues to trustworthy information transfer. Processes and procedures should be adopted in relation to the value to the organization of the information being transferred.

2.2.3.2.4 Availability

Availability is about ensuring that the information is available when it is required by an authorized user. Loss of information could be interpreted as being just as significant as fraudulent modification. It may be necessary to demonstrate that specific information is still available for a legally stipulated time after transfer. In this area, topics such as regular backup and business continuity planning are critical. These topics are dealt with in BIP 0008-1.

Procedures and processes should be implemented that ensure that the electronic information is available as required. This is best implemented by storing information electronically transferred in compliance with BIP 0008-1.

KEY ISSUE

> Ensuring that information is available when required is a key requirement.

2.2.3.3 Security management guidance

Publications are available that provide advice in devising comprehensive sets of information security guidelines to meet the organization's needs. These guidelines should be included in the organization's review process. For some applications, the adoption of externally accredited security schemes as additional confirmation of compliance to their security policy may be appropriate.

There are a number of national and international standards that, if implemented, should support the organization's demonstration of duty of care (see next 'Comment' box). Standards that cover information security and service quality issues are particularly appropriate.

COMMENT – Information security management standards

The internationally accepted information security management standards are:

- BS ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*;
- BS ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*.

There are other publications in the ISO/IEC 27000 series that may also be applicable in specific applications.

Information is the lifeblood of all organizations and can exist in many forms. It can be stored electronically and transmitted by mail or by electronic means. In the competitive business environment, such information is constantly under threat from many sources. These can be internal, external, accidental or malicious.

These information security management standards address these issues and have thus been implemented in many major organizations. They are referenced in many places and are becoming the common benchmark against which information security is measured.

Within the UK, there is a formal certification scheme against the requirements of BS ISO/IEC 27001. A number of UK and overseas organizations have seen the benefit of compliance, particularly where they offer IT services to other organizations. Other organizations have used the two documents to assess their information security management systems, as part of their risk assessment processes.

It is important that any decisions made concerning certification or compliance with the standards are recorded by the organization.

KEY ISSUE

> Where an appropriate national or international standard is implemented, electronic transfer systems should be included within the scope of compliance with the standard

2.2.3.4 Scope

To fulfil the duty of care objective, the organization needs to action the following.

Topic	Content	Section of BIP 0008-2
Information security policy	Implement an information security policy	2.2.3.5
Risk assessment	Carry out a risk assessment and implement appropriate recommendations	2.2.3.6
Information security infrastructure	Develop, implement and test an information security management system	2.2.3.7
Third-parties	Develop policies and procedures for working with third-parties	2.2.3.8
Access rights	Manage access to transfer systems using access controls	5.15.2
Business continuity planning	Develop, implement and test a business continuity plan	5.15.3

Table 3 – Information transfer duty of care

2.2.3.5 Information security policy

All information that is in the process of electronic transfer is vulnerable to loss or change, whether accidental or malicious. To protect such information, appropriate security measures need to be implemented to reduce the risk of a successful challenge to its authenticity.

Information security, whether in the area of confidentiality, integrity or availability (see 2.2.3.2), is not simply a constraint to be placed upon computer systems. Security and access to the physical environment (e.g. buildings and networks) and the implementation of policies and procedures by all staff are key elements.

The organization should adopt an information security policy for electronic transfer (sending and/or receiving as appropriate).

Where the organization has an information security policy for other processes (for example, storage), then it should be extended to incorporate the requirements of the electronic transfer systems within its scope.

The information security policy document should contain (for the electronic transfer systems), as a minimum:

- the scope of the information security policy;
- a statement of the management objectives regarding information security for electronic transfer (sending and/or receiving as appropriate);
- specific policy statements;
- requirements for different information classification categories;
- definition and allocation of electronic transfer responsibilities;
- electronic transfer training and awareness requirements;
- policy for dealing with potential or actual compromise of electronic transfer systems;
- policy regarding compliance with appropriate standards; and
- approval and review process.

The information security policy should be approved by the organization's top management. The organization should then agree and document appropriate levels of security for managing its information transfer systems, in compliance with its stated information security policy.

KEY ISSUES

> Develop, authorize and implement an information security policy.

> Ensure that the policy's scope includes the information transfer systems

2.2.3.6 Risk assessment

Information security measures are often applied piecemeal, reacting to security incidents or to available computer software tools. This type of approach can fail to recognize the value of the information asset and the risks to the organization from security compromise during electronic transfers. This may leave gaps in security, which may be filled only at some later date after a security breach.

A more structured approach is to review the information assets and assign risk factors (based on asset value, system vulnerability and likelihood of attack). The security policy can then be produced and approved against the value model.

The organization should undertake an information security risk assessment aligned to the electronic transfer systems, and record the results. BS ISO 31000 provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. It can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Existing security measures should be reviewed for effectiveness. Factors such as the balance between the cost of implementation and the security achieved should be taken into consideration during the review process.

Where different types of electronic transfer system can be used, their individual impact on the risk assessment results should be reviewed.

KEY ISSUE

> Perform a risk assessment of existing security measures, and implement cost-effective technology and/or procedures to fill any gaps found.

2.2.3.7 Information security infrastructure

In order to control and manage security issues with electronic transfer systems, a management infrastructure needs to be implemented, including relevant electronic transfer systems within its scope. The infrastructure should have as its objectives:

- approval and review of the information security policy;
- monitoring of threats to information security;
- monitoring and review of security breaches; and
- approval of major initiatives to enhance information security.

KEY ISSUE

> Plan and implement an information security framework.

2.2.3.8 Third-parties

All information that is being transferred via a third-party is potentially vulnerable to loss or change, whether accidental or malicious. To protect such information, appropriate security measures need to be implemented to minimize the risk of such a loss or change, and thus a successful challenge to its authenticity.

Where the third-party is retaining transferred information for a period, however short, it should have adopted an information security policy in relation to this information. This policy may need to be incorporated within, or referred to by, the organization's own information security policy; this means the third-party will be formally 'trusted'.

Where the trusted third-party (TTP) has an information security policy for other processes (for example, storage), the use of electronic transfer should be incorporated within its scope.

INFORMATION

SSL/TLS are used to encrypt internet traffic; a similar cryptographic approach is used to authenticate another system or database connection known as Secure Shell (SSH).

SSH is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, file transfer and other secure network services between two systems via a secure channel over an insecure network.

SSH frequently uses Public/Private Key pairs and, as with other cryptographic techniques, key management can become an onerous task but is one that cannot be ignored as inappropriate access to a Private Key can cause major compromise to information availability, authenticity or integrity.

The standards for SSH are documented in Internet Engineering Task Force Request for Comments (IETF RFCs) which are listed at http://datatracker.ietf.org/wg/secsh/documents; there is also useful information at OpenSSH, www.openssh.com.

EXAMPLE

One area that TTPs will frequently have covered in their security policy is that electronic transfer with them should be over secure, encrypted channels. This will prevent eavesdropping on the message and will allow them to authenticate the identity of the person or system accessing their systems. This will frequently use either SSL or TLS (see below).

Such use of a secure channel is also often used for secure mail applications or access to webmail services. A number of secure email services are based on the approach of sending links to messages held on secure web servers, using normal email services. Recipients follow the links using their browser and will only be able to access the confidential messages over an SSL or TLS protected channel, which will only be opened up to them when they have successfully identified themselves as the intended recipient. Note though that such secure channels may mean that information may not be checked by the organization's boundary defences intended to prevent access to inappropriate or dangerous material.

DEFINITIONS – SSL and TSL

SSL is short for 'Secure Sockets Layer', a protocol for confidential transmission across the internet. SSL works by using a Private Key to encrypt data that are transferred over the SSL connection. Most browsers support SSL and many websites use the protocol to obtain confidential user information, such as credit card numbers. Normally, URLs that require an SSL connection start with https: instead of http:

SSL creates a secure channel connection between a client and a server, over which any amount of data can be sent securely. This protocol is standards approved by the Internet Engineering Task Force (IETF).

SSL is being superseded by TLS (Transport Layer Security), which is an extension of SSL. TLS is a newer protocol for privacy and data integrity between client and server applications communicating over the internet.

The TLS protocol is made up of two layers:

1. the TLS Record Protocol – it ensures that the connection is private by using symmetric data encryption, and it ensures that the connection is reliable. The TLS Record Protocol is also used for encapsulation of higher level protocols, such as the TLS Handshake Protocol;
2. the TLS Handshake Protocol – it allows authentication between the server and the client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

TLS and SSL are not interoperable.

Whilst SSL continues to be referred to and used it should be noted that TLS offers enhanced security over SSL. Frequently where TLS is actually in use it is often referred to, somewhat erroneously, as SSL.

Where a third-party provides transfer services (for example, where a service provider manages an EDI system), such services should be included within the scope of compliance with the Code. Services should include appropriate recovery and disaster recovery processes.

The provider of third-party services needs to be aware of the value of the service that it provides, and needs to execute its responsibility under the 'duty of care' principle.

To fulfil this objective, the provider of third-party services should ensure that it:

- is aware of legislation and regulatory bodies pertinent to itself and to its client's industry sector;
- is aware of legislation pertinent to countries (or other geographical areas) where its services are delivered;
- establishes a chain of accountability and assigns responsibility for activities involving transfer services at all levels;
- keeps abreast of developments by keeping in contact with the appropriate bodies and organizations; and
- is aware of any legislative or regulatory control of trusted third-party services.

Similarly, and reciprocally, the organization should ensure that the third-party:

- is aware of legislation and regulatory bodies pertinent to the trusted third-party's industry;
- is aware of legislation pertinent to countries (or other geographical areas) where its services are delivered;
- establishes a chain of accountability and assigns responsibility for activities involving transfer services at all levels;
- keeps abreast of developments by keeping in contact with the appropriate bodies and organizations; and
- is aware of any legislative or regulatory control of trusted third-party services.

Where appropriate, organizations should request documentation that demonstrates the third-party's duty of care, as part of the agreed contract.

KEY ISSUES

> When transfer systems use third-party resources, the third-party should only be considered to be 'trusted' where it has an appropriate information security policy.

> Where a third-party provides transfer services, such services should be included in the organization's information security policy.

2.3 Roles and responsibilities of workers

It is important when developing policies and procedures to ensure that:

- information related to the policies and procedures is made available to those who are or may be affected by them;
- there is a mechanism for feedback from the implementers of the policies and procedures;
- there is a mechanism for reviewing risks related to the policies and procedures;
- details of any challenges to the authenticity and/or integrity of stored information is fed back to those responsible for compliance with the Code; and
- key individuals within the organization responsible for managing such communications are identified.

KEY ISSUE

> Ensure that a reporting and communications mechanism is in place, to ensure that new or updated policies and procedures are implemented by all appropriate staff.

2.4 Legal and regulatory environment

This topic is discussed in Annex H of BIP 0008-1.

3 Planning

3.1 Actions to address risks and opportunities

3.1.1 General

This section of the Code relates to Clause 6 of BS 10008, 'Planning'.

When planning for the management of the authenticity and integrity of information during transfer, the organization needs to consider the issues referred to in 1.2 and the requirements referred to in 1.3 and determine the risks and opportunities that need to be addressed to:

a) ensure the information transfer system can achieve its intended outcome(s);
b) prevent, or reduce, undesired effects; and
c) achieve continual improvement.

The organization also needs to plan:

a) actions to address these risks and opportunities; and
b) how to:
    1. integrate and implement the actions into its information transfer system processes; and
    2. evaluate the effectiveness of these actions.

3.1.2 Risk assessment

Information transfer procedures are often developed in an unstructured way, by reacting to user requirements, security incidents and/or to available computer software tools. This approach on its own can easily leave gaps in information transfer, which are only filled at some later date, typically after a security breach. A more structured approach is to review the information assets of the organization and assign risk factors (based on asset value, potential threats, system vulnerability and likelihood of attack), on the basis of which appropriate, cost-effective information transfer procedures can be identified. An essential part of information transfer is the implementation of an appropriate security policy, which should be produced and approved based on the risk assessment, and against which security measures can be developed and implemented.

NOTE: A review of this type generally requires security expertise and a range of appropriate technical skills.

The organization should undertake an information security risk assessment along these lines, and document the results obtained. Of particular importance are the security measures implemented to control the information transfer. The risk analysis needs to include vulnerability risk factors consistent with the type of transfer protocol used.

On the basis of the results of the risk assessment, existing security measures should be reviewed for effectiveness. Factors such as the balance between the cost of implementation and the security achieved need to be taken into consideration during the review process. Where the review indicates that changes to security measures are appropriate, an action plan should be drawn up with new or amended security measures prioritized for implementation.

KEY ISSUE

> Perform a risk assessment of existing security measures, and implement cost-effective technology and/or procedures to fill any gaps found.

The risk assessment will lead to the acquisition of information and the creation of risk reports. These reports, backed up by the information used to develop the conclusions and recommendations in the reports, may provide useful evidence in relation to information transfer decisions made by the business.

It is thus important to retain information related to risk assessments in line with an information retention schedule.

KEY ISSUE

> Retain records of risk assessment methods and results in line with the retention schedule.

3.1.3 Risk treatment

The results of the risk assessment should be used to guide and determine the appropriate management action and priorities for managing information risk and implementing controls in order to protect against those risks.

ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

ISO/IEC 27005 describes the input to a risk treatment process as a list of identified risks, prioritized according to the organization's risk evaluation criteria. Risk treatment includes the identification and implementation of controls to reduce, retain, avoid or share the identified risks.

Risk treatment can be implemented by one or more of the following non-exclusive processes:

- risk modification;
- risk retention;
- risk avoidance;
- risk sharing.

Risk modification involves the addition, removal or modification of existing controls so that the residual risks can be re-evaluated.

Risk retention is the process of retaining an identified risk without further action. This is acceptable when the identified risk is within the agreed risk criteria.

Risk avoidance involves the removal of processes related to the risk, so that the risk is no longer present. This may be used when the cost of other forms of risk treatment are too costly to implement.

Risk sharing involves the sharing of the identified risks with other parties, such as by insurance or by subcontracting particular processes.

3.2 Objectives and achievements

The organization needs to establish information transfer objectives at relevant functions and levels.

The information transfer objectives need to:

- be consistent with the information transfer policy;
- be measurable (if practicable);
- take into account applicable information transfer requirements, and results from risk assessment and risk treatment;
- be communicated; and
- be updated as appropriate.

The organization shall retain information on the information transfer objectives.

When planning how to achieve its information transfer objectives, the organization needs to determine:

- what will be done;
- what resources will be required;
- who will be responsible;
- when it will be completed; and
- how the results will be evaluated.

4 Support

4.1 Resources

This section of the Code relates to Clause 7 of BS 10008, 'Support'.

The organization needs to determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information transfer system.

4.2 Competence

The organization needs to:

- determine the necessary competence of person(s) doing work under its control that affects its information transfer performance;
- ensure that these persons are competent on the basis of appropriate education, training, or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- 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 workers; or the hiring or contracting of competent persons.

4.3 Awareness

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

- the information transfer policy;
- their contribution to the effectiveness of the information transfer system, including the benefits of improved information transfer performance; and
- the implications of not conforming with the information transfer system requirements.

4.4 Reporting and communications

It is important when developing policies and procedures to ensure that:

- information related to the policies and procedures is made available to those that are or may be affected by them;
- there is a mechanism for feedback from the implementers of the policies and procedures;
- there is a mechanism for reviewing risks related to the policies and procedures;
- details of any challenges to the authenticity and/or integrity of transferred information is fed back to those responsible for compliance with the Code; and
- the methods used for these communications are regularly assessed for effectiveness, and updated where necessary.

KEY ISSUES

> Ensure that a reporting and communications mechanism is in place, to ensure that new or updated policies and procedures are implemented by all appropriate workers.

> This documentation should be retained in compliance with the retention schedule.

KEY ISSUE

> Retain documentation related to reporting and communications procedures in line with the retention schedule.

4.5 Documented information

4.5.1 General

Documented information (also known as records) related to the process of managing information transferred electronically needs to be created and retained for as long as is necessary. Section 4.5.2 details procedural documentation that needs to be created and retained. This section also includes information related to the management of this information, including the requirement for version control and appropriate retention periods.

4.5.2 Procedural documentation

4.5.2.1 General

Compliance with the Code requires the availability and use of specified documentation. This documentation consists of the:

- information transfer policy statement (see 2.2.2);
- information security policy document (see 2.2.3);
- procedures manual (see 4.5.2.3); and
- system description manual (see 4.5.2.4).

The availability of these documents, and demonstrable adherence to the procedures described therein, should, if effectively constructed, provide the audit trail that may be used to demonstrate the authenticity of transferred information, and thus enhance its evidential weight.

Note that each of the documents mentioned above may actually be maintained as multiple documents, or may be combined. The key recommendation is that the documentation exists, is maintained, and is readily accessible to those authorized within the organization to access it and to any authorized third-party who may require access. It may also be appropriate to use the documents created in accordance with BIP 0008-1, and extend them to cover the recommendations of this part of the Code.

All documentation needs to be maintained in line with existing working practices, and thus should be maintained under a version control system (see 5.3).

Additional documentation may be required to support the daily operation of the system, for example:

- a system maintenance log (see 5.14);
- an audit trail (see 4.5.3); and
- compliance statements (see 6.3.4).

The content of the documentation described above can easily become unreliable where there are no procedures in place to ensure that they keep pace with both organizational and system changes. Unreliable documentation may adversely affect legal arguments relating to the correct operation of an information transfer system. It is, therefore, important to ensure that the definitive versions of system documents are brought under configuration management control, and are firmly linked to the organization’s change management procedures.

Where compliance with the Code is claimed over a period of time during which different editions of the above documentation were appropriate, then all editions of this documentation should be kept, in

conformance to the policy statement. This is to ensure that, where information regarding the system at a point in the past is required, it can be obtained from this document store.

KEY ISSUE

> Documentation is essential evidence as to the policies, procedures and technology used. It is part of the system audit trail.

4.5.2.2 Updating and reviews

It is important to ensure that the procedures implemented at any time during the storage life of any specific piece of information that has been transferred can be determined. This is achieved by ensuring that the procedures manual (see 4.5.2.3) is kept up to date, and that all previous versions are kept in compliance with the policy statement (see 2.2.2).

KEY ISSUES

> All changes to operational procedures should be managed by a change control procedure, and include updating the procedures manual.

> Current and superseded versions of the procedures manual should be kept in compliance with BIP 0008-1.

> The procedures manual should be regularly reviewed, to ensure that it is up to date.

> All changes should be reviewed to ensure that compliance with the Code is not compromised.

4.5.2.3 Information transfer procedures

The organization should maintain a procedures manual, which should document (or reference) procedures used for operating the electronic transfer system, to ensure its conformity to the controls detailed in the Code.

Where an organization operates a quality management system, such as BS EN ISO 9000, the procedures manual should be included within the quality system.

KEY ISSUE

> A procedures manual should be made available, containing details of (or reference to) other relevant documentation concerning all procedures relevant to the electronic transfer system.

The procedures manual should include the topics listed in Table 4.

Topic	Content	Section of BIP 0008-2
Standardized documents	Using templates and other skeleton documents	5.2
Version control	Management of multiple versions of a document	5.3
Sending data to archives	Sending data to archives	5.6
Preparation for transfer	Ensuring the appropriate documents are prepared for transfer	5.7
Transfer	Transferring the electronic documents	5.11
Receipt of transfer	Capturing the information received	5.12
System maintenance	Physical equipment maintenance	5.14
Security and protection	Complying with the information security policy	5.15
Contracts	Managing the exchange of contracts	5.16
Third-parties	Working with third-party systems	5.17

Table 4 – Procedures manual topics for information transfer

4.5.2.4 Key technology components

A description of hardware, software and network elements that comprise the electronic transfer system is required. This should include details of system configuration. The documentation should be structured so that details of the system at any time during the period of its use may be readily accessed. This may be achieved by creating a new version of the manual every time there is a change, or by including a 'change control' section in the manual. What is important is that there is a clear description of the system as it was at a particular time in the past; without this it will be difficult to explain how a particular information transfer was implemented at that time.

For systems already in operation, information transferred by the system prior to the introduction of the Code cannot be considered as meeting its provisions unless the controls and procedures described in the Code have been in place from the time of transferring that information.

Where the information transfer policy requires compliance with particular national and/or international standards, the system description manual should include a section demonstrating compliance with those standards. This enables system auditors to check the performance and reliability of the system against these standards.

KEY ISSUES

> A system description manual should be made available, containing details of (or reference to other relevant documentation containing details of) all technology-related issues relevant to the electronic transfer system at any point in time.

> Document any compliance to standards methodology implemented.

The system description manual should include the topics listed in Table 5.

Topic	Content	Section of BIP 0008-2
Transfer initiation	Processes for initiating transfers	5.7.2
Integrity checks	Processes that ensure the integrity of transferred information	5.7.8
Identity authentication	Processes for identifying the sender and recipient of a document	5.8
Sender and recipient authentication	Authenticating the identification of sender and recipient	5.9
Identification of information	Ensuring that transferred information is correctly identified	5.10
Systems	Details of the systems in use	5.11.1
Interim or temporary information storage	Storing information prior to writing it to final storage	5.11.2
Confirmation of receipt	Dealing with confirmation of receipt	5.12.7
Access rights	Configuration of user access management tools	5.15.2
Time considerations	Dealing with time issues	5.18
Error handling processes	Dealing with errors in transfer systems	5.19

Table 5 – Information transfer system description manual topics

4.5.3 Audit trails

4.5.3.1 General

When preparing information for use as evidence, it is often necessary to provide further supporting information. This information may include details such as date of transfer of the information, details of movement of the information from medium to medium, and evidence of the controlled operation of the system. These details are known as ‘audit trail’ information.

This audit trail information is needed to enable the working of the system to be demonstrated, as well as the progress of information through the system. Audit trails need to be comprehensive and properly looked after, as without them the integrity and authenticity, and thus the evidential weight, of the transferred information could be called into question.

4.5.3.2 Purpose

The audit trail as defined for the Code consists of the aggregate of the information necessary to provide a historical record of all significant events associated with the transferred information. As such it covers the answers to all the classic questions concerning the provenance of any electronic information that has been subject to electronic transfer:

- Who?
- What?
- Where?
- When?
- Why?
- How?

These audit trail details can be split into three categories:

1. system (including the hardware platform(s), applications and operating software, configuration, and processes and procedures);
2. transferred information;
3. stored information (see BIP 0008-1).

In most organizations, the audit trail will consist of a collection of system- and operator-generated logs.

It is essential that system clocks be synchronized with an accurate time source to ensure that times recorded in audit trails are consistent and reliable.

4.5.3.3 Generation

Audit trail data should, as far as practicable, be generated automatically by the system, and the system description manual (see 4.5.2.4) should describe the processes. In this case, the data should be created and stored immediately following the event that is being audited.

Where audit trail data are not generated automatically by the system, procedures for its manual (or other) generation should be implemented. In this case, the data should be created as soon as possible after the event that is being audited. For example, if the record is of when an operator of an electronic transfer system started work, the time should be recorded before work actually starts. If the record is of when preparation of a particular batch of electronic documents was started, the time should be recorded just before the preparation of that batch commences.

It should not be possible to amend any audit trail data. Deletion should only be possible in accordance with the organization's retention policy.

KEY ISSUE

> Audit trail data should be generated automatically wherever possible. It should not be possible to alter audit trails.

4.5.3.4 Audit trail content

4.5.3.4.1 General

The audit trail content is critical, as it can be used to audit such activities as the preparation and sending and receiving of electronic transfers. Thus, the audit trail needs to include a record of all relevant activities related to the systems. If any significant activity is not audited, then the whole audit trail can be discredited and, as a direct result, all or any electronic transfers will also be able to be discredited.

Thus, technologies for providing electronic transfer systems should be chosen with audit trail requirements in mind. This may result in technologies being rejected that may otherwise have appeared suitable for a particular application.

KEY ISSUE

> When choosing electronic transfer systems, consider suitable audit trail functionality as a basic system requirement.

4.5.3.4.2 Transferred information

Records should be kept of historical activities or events that may need to be reconstructed in the future, as additional evidence to support transferred electronic documents.

Audit trails should contain the sufficient and necessary information to provide evidence of the authenticity of transferred electronic documents.

The audit trail should contain the following information where relevant:

- time when the electronic transfer was initiated;
- time when the inbound receipt was effected;
- time when the personal receipt was effected.

In some applications, a requirement for confirmed, trusted time stamps is key. Such information should be recorded in the audit trail.

4.5.3.4.3 Route details

The audit trail should contain the following information where relevant:

- transfer initiator (person or application);
- initiation hardware;
- transfer server;
- protocols used;
- carrier(s) used;
- receiving server;
- transfer receiver (person or application).

4.5.3.4.4 Storage requirements

Where there is a requirement for intermediate storage, sufficient audit information should be stored to enable such time and route details as are required to be made available.

KEY ISSUE

> Store sufficient related audit trail information to ensure that time and route details can be determined.

4.5.3.4.5 Date and time

Each audit trail data record should have an associated date and time that relates to the date and time of the electronic transfer event. This information should be sufficiently accurate that a subsequent investigation can determine the train of events.

The date and time will normally be that of the creation of the audit trail data, but if this creation is made essentially contemporaneously with the event that is being audited, the time will be, to all intents and purposes, that of the event itself.

Where a date and time stamp is applied automatically by the system, all changes to the system clock should be recorded in the audit trail. Such changes need to be suitably authorized and it may be necessary to adjust for daylight saving time or inaccuracy of the clocks.

Where the actual time that an event occurred is important, the use of trusted time should be considered (see 5.18).

It may be appropriate to link audit information to the information to which it refers, by the use of digital signatures, or MACs or other forms of cryptographic checksums.

KEY ISSUE

> Ensure sufficient accuracy of date and time for the application in question.

4.5.3.5 Security of audit trails

4.5.3.5.1 General

The audit trail needs to be secure. If an audit record can be maliciously or inadvertently altered or counterfeited, then the whole audit trail may be discredited and as a direct result, all or any transferred information held within the system may also be able to be discredited.

4.5.3.5.2 Access

Audit trail information will need to be accessed by authorized operators at relevant times. In some applications, access may only be needed on an ad hoc basis, and thus it is important that the access and interpretation procedures are documented.

There should be procedures for the secure management of audit trail access and interpretation.

Audit trail data should be available for inspection by authorized external personnel (such as auditors) who have little or no familiarity with the system.

Access to the audit trail should, itself, be audited.

KEY ISSUE

> Keep audit trails secure, with audited access only.

4.5.3.5.3 Integrity and protection

If the authenticity of transferred electronic documents is questioned, the integrity of the audit trail may be fundamental in establishing the authenticity, and thus the evidential weight, of this information. If the possibility exists that the audit trail data could be modified, this will reduce the evidential weight of any information to which these records apply.

The audit trail should be kept at the level of security appropriate to preventing any change to any data within it, and in accordance with the organization's information security policy (as well as the retention policy).

The audit trail should be subject to equivalent internal records management policies and procedures as other 'vital records' of the organization.

Secure backup copies of the audit trail should be kept, including automated and manual audit trail data.

Where file recovery procedures have been implemented as part of the transfer systems, sufficient audit trail data should be stored to demonstrate that the recovery did not affect information authenticity.

For least risk, store audit trail data on 'write-once-read-many' (WORM) media. If a rewritable medium is used, then additional procedures need to be implemented to prevent changes being made. The use of magnetic tape will make it relatively difficult to modify data, as magnetic tape is normally a serially written medium.

If audit trail data have been modified, then any such modification should be audited.

Paper documents used for audit trail data should be removed frequently from the place of use and stored securely. The longer a document used for audit trail data (e.g. operator logs) is left in a relatively insecure place, for example, at a workstation, the higher the risk of tampering. Users need to assess such risk when using paper for audit trail records. Where paper documents are used, electronic copies of them should be stored on an information management system (in accordance with BIP 0008-1).

KEY ISSUES

> Wherever possible, store audit trail data in an unmodifiable form.

> Where this is not possible, use security measures to ensure that it is not modified.

4.5.3.6 Management

The audit trail needs to be properly managed, as it may be of critical importance to the organization. All claims of compliance with organizational policies may be discredited if the audit trail is not treated correctly and cannot be interpreted unambiguously.

KEY ISSUE

> Ensure that the audit trail data are authentic, accessible, sufficiently comprehensive and understandable.

4.5.3.7 Storage and retention

The storage of audit trail data is a topic often not included in an organization's electronic storage policies. As they are frequently created automatically, and infrequently accessed, they are usually forgotten and thus not subject to adequate control.

To ensure that all relevant audit trail data are stored, 'audit trail data' should be included as a specific information 'type' in the policy document. It should be stored for at least as long as the information to which it refers is stored.

Some systems control the size of audit trail data files by the use of 'looping', which sets the maximum size for the data file, and when this size is reached, new data overwrites the oldest data in the file. Thus, old audit trail data are lost. This process may not be in conformance to required retention periods.

There should be procedures that identify circumstances when an audit trail data file becomes full and the action to be taken to retain data as required by the retention policy.

Where an organization is working within a BS EN ISO 9000 environment, audit trail data relating to compliance with the quality management system are typically destroyed after a short period of time. This is not the case with audit trail data from electronic transfer systems, which should be stored for the same period as that of the data to which they relate.

KEY ISSUE

> Ensure that audit trail data are retained for at least the same period as that of the data to which they relate.

4.5.3.8 Format

Frequently, when an organization wants to automate its computer operations environment, it makes use of operating system logs to monitor the system for specific events or error conditions.

At an application level, ensuring that the application provider uses standard error messages, typically agreed with the organization during the design stage, also enables application status conditions to be monitored.

For example, if an application reads invalid data from a file, rather than just aborting the program with nobody aware of what has happened (until the users raise a support call), if the program writes a status message to an error/system log, in an agreed format, the monitoring software will detect this and notify the user and/or support staff.

These notifications are an important trigger to investigate the continued, proper operation of the system. The entries into the error system log that caused the monitoring software to raise the alert should be part of the audit trail and should be controlled in accordance with the Code.

KEY ISSUE

> Use audit trail formats that enable easy interpretation, both by system users and by automated monitoring tools.

4.5.3.9 Access and interpretation

Access to audit trail information needs to be controlled. In some applications, access may only be needed infrequently, and thus it is important that the interpretation procedures are documented. As audit trail data may be inspected by authorized external personnel (such as auditors) who have little or no familiarity with the system, interpretation procedures should be understandable by non-technical users.

There are frequently a number of departments (or individuals) within an organization (or external to the organization), including those representing user, audit and legal functions, that may need access to specific parts of audit trail information. This access should be controlled, to reduce the possibility of compromise.

Access to the audit trail should itself be recorded in the audit trail.

KEY ISSUE

> There should be documented procedures that are followed when audit trail data needs to be accessed and interpreted.

5 Operation

5.1 Management overview

This chapter deals with the procedures and processes (automated where appropriate) that need to be implemented as part of an electronic transfer system. This will enable the demonstration to internal or external parties that procedures and processes that conformed to the Code were in operation at the appropriate times. The actual procedures implemented are to be documented in a procedures manual.

5.2 Standardized documents

Organizations may use 'skeleton' documents or 'templates' for the creation of personalized documents for transfer purposes. Where it is likely that there may be a challenge to the authenticity of such a document, the sender should be able to reconstruct the transferred document. This requires that the original skeleton or template is stored, together with information regarding the version used for any particular created document.

Where standardized documents are modified and transferred, the original documents should be held in compliance with BIP 0008-1. The content of these documents should be managed using a version control system, to enable appropriate records to be kept of changes made to these documents.

All versions of such documents should be stored in accordance with the organization's retention policy.

COMMENT – XML schemas

XML schemas (see 5.7.9) effectively address the same inter-organizational interoperability requirements as the standards used in EDI, such as Electronic Data Interchange For Administration, Commerce and Transport (EDIFACT).

It is quite acceptable for trading partners mutually to agree to a private EDI format or XML schema; however, if they choose to do so there is an ongoing documentation and maintenance task that is likely to be an unproductive use of resources.

EDI standards:

United Nations/Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) is the international EDI standard developed under the United Nations.

EDIFACT can use XML – ISO/TS 20625:2002, Electronic data interchange for administration, commerce and transport (EDIFACT) – Rules for generation of XML scheme files (XSD) on the basis of EDI(FACT) implementation guidelines.

Other EDI schemas exist such as ebXML (Electronic Business using eXtensible Markup Language, as specified in the ISO/TS 15000 series), and RosettaNet (www.rosettanet.org).

KEY ISSUE

> Where templates/skeleton documents are used, they should be managed and stored using the same procedures as the documents on which they were based during their creation.

5.3 Version control

All hardware, software and procedural documentation used in conjunction with the Code should be maintained under a version control system.

Such systems should include the keeping of appropriate records of changes made and should enable relevant information about the configuration of the electronic transfer system at any time in the past to be reviewed.

KEY ISSUE

> Keep records of all procedural and process documentation in accordance with a retention policy. This is to enable the configuration and use of the system at any point in the past to be demonstrated.

5.4 Change control

Where changes to automated processes are made, an appropriate change control procedure should be followed. Such processes should be tested prior to live implementation and audited. Records should be retained that demonstrate the proper implementation of change control procedures.

EXAMPLE

Where script changes for automated file transfers are implemented, the new scripts should be fully tested prior to their implementation.

KEY ISSUE

> Keep records of all procedure and process changes, including an audit trail of testing and implementation.

5.5 Storage

The electronic information that is to be transferred or that has been received by transfer should be stored in accordance with BIP 0008-1 along with any associated metadata (e.g. agreed data file format, unique electronic transfer identity, time and date stamp, index, sender and intended recipient identity and address, digital signatures, certificates and/or receipt confirmation information).

The sender also should subsequently store any receipt confirmation information associated with the transferred document in accordance with BIP 0008-1.

Similarly, the recipient should store the received transfers in accordance with BIP 0008-1.

EXAMPLE

The retention requirements of the sender and the recipient of a message may be completely different. This is because the value of the transaction may be completely different to each. For example, the message confirming the receipt of an order of a car is a commonplace event for the motor dealer, but not for the purchaser.

KEY ISSUE

> Electronic storage should be in compliance with BIP 0008-1.

5.6 Sending data to archives

5.6.1 General

Technologies used for the initiation and control of transfer of electronically transferred information between the organization and an archive, whether the archive is operated in-house or by a third-party service provider, should be documented.

There are three main approaches to the archiving of electronically transferred information:

1. send every data file to the archive at the same time as it is sent to the recipient, or when a confirmation of receipt is received;
2. send the data file to the archive, for them to forward it to the ultimate recipient (this is sometimes called an 'online notary');
3. send an accumulated set of data files to the archive at a later point in time from either sending or confirmation of receipt.

COMMENT

Where a notary service provider is used, it should be in compliance with the Code for each of the separate transfers (the first between sender and notary, the second between notary and recipient).

Such capabilities as provided by these approaches may be used selectively. Where proof of authenticity of the identity of sender and/or recipient is required, cryptographic controls (e.g. digital signatures) will frequently be used.

The method of ensuring that received and subsequently stored electronic information is identical to that originally sent should be documented. Such integrity checks should include situations where the data files have been moved from one storage device to another, and where recovery from system failure has occurred.

KEY ISSUE

> Technologies used for managing the transfer of information to electronic archives should be documented.

5.6.2 Procedures

Procedures that should be followed when preparing data files for archiving should be documented. This documentation should include details of procedures carried out within the organization or at a third-party archive service provider. This documentation should include procedures for the identification of data files to be transferred to the archive.

These conventions should be defined to enable unambiguous subsequent retrieval that may be many years later. Such naming may by necessity, involve date/time, in which case consideration should be given to the uniqueness of such (e.g. time zones or daylight saving time).

The documentation should include the following procedures for file transfers to the archive:

- version control of data files – care needs to be taken when a document with the same historical base has been modified or approved by different parties, or at different times;
- anti-virus controls on data files;
- approved file formats of data files – where procedures vary depending upon the data file format, each procedure should be documented, together with a procedure which ensures that the correct procedure has been implemented;
- retention periods of data files – this should clearly differentiate between retention and destruction requirements.

The documentation should also include procedures for the use of the following with data files to be transferred to the archive:

- encryption and/or compression;
- digital signatures or other authentication processes.

KEY ISSUE

> The electronic transfer of information to archives should be performed in a controlled manner, taking into account any longevity issues such as long-term format accessibility issues.

5.7 Preparation for transfer

5.7.1 General

The procedures described in this section are those that should be followed by the sender of an electronic transfer.

Procedures used to prepare electronic information for transfer should be documented. Such procedures may be used, for example, to increase integrity, confidentiality and authenticity, and/or speed of transfer.

Where several transfer techniques are employed, particular attention should be paid to ensure that the required technique is used in accordance with the policy document.

The use of industry standard software should be considered in all cases, to reduce the risk of file corruption and irretrievability of the transferred information.

5.7.2 Transfer initiation

The effective transfer initiation time for electronic information is when it starts to leave the sender in electronic form. The sender may be an individual, a business unit, the application or device that originated the electronic information. Where transfer is between organizations, the sender should be unambiguously linked to the originating organization, and the initiation time is when the document is transferred by the organization.

The processes used to record when electronic transfer is initiated should be documented. A time and date stamp should be added to the document at the time of transfer and transferred with the document.

NOTE: A date and time stamp from a PC on a network is unlikely to be the actual transferred time unless it is connected to the carrier directly.

In some electronic transfer systems, especially those with very large information transfers, it may also be necessary to record when transfer was completed (this may not be related to the time when the information was received by the recipient).

Where the 'actual' time of a transfer event is important, the use of 'Trusted Time' should be considered (see 'Definition').

DEFINITIONS

Trusted Time is time that is certified to be traceable to the legal time source for the application in which it is being used and is not forgeable either at the time of initial use or anytime in the future.

RFC 3161 (and RFC 5816) are the IETF Public Key Infrastructure (PKI) Time Stamping Protocol specifications (www.ietf.org/rfc/rfc3161.txt) which are extended in ANSI X9.95:2012 for the management and security of trusted time stamps (www.ansi.org)

RFC 3161 describes the format of a request sent to a Time Stamping Authority (TSA) and of the response that is returned. It also establishes several security-relevant requirements for TSA operation, with regards to processing requests to generate responses.

A time-stamping service supports assertions of proof that a datum existed before a particular time. A TSA may be operated as a Trusted Third-Party (TTP) service, though other operational models may be appropriate, for example, an organization might require a TSA for internal time-stamping purposes.

Another useful source is the technical specification published by the European Telecommunications Standards Institute (ETSI) entitled Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities (ETSI TS 102 023).

Where a break in transfer occurs that requires operator intervention, the reconnected time and date may also need to be recorded and transferred.

KEY ISSUE

> Processes used in the initiation of transfers should be documented. The process for the addition of time of initiation should be included.

5.7.3 Malicious software

Malicious software, such as viruses, macro viruses, worms and Trojan horses, are a major hazard to electronic transfers (see also 5.12.2).

COMMENT – Malware

Malware (such as viruses, Trojan horses and worms) can wreak havoc on information stored in computer systems and on the integrity of information transferred between systems; it can also change the behaviour of previously well-controlled and understood transfer systems. It may also prevent such systems from operating at all.

The cost of protection against and recovery from malware can be significant, but the effect of having no protection can be disastrous.

You should warn the organizations with whom you communicate that it is their responsibility to check for viruses, etc., but if they become aware that you have not had reasonable preventive measures implemented effectively then they may, justifiably, regard your organization as liable for the costs of damage recovery. At the very least they may terminate a trading agreement or generate reputationally damaging adverse publicity for your organization.

Procedures that reduce the possibility of computer viruses and other malicious software being included within information to be transferred should be documented.

KEY ISSUE

> To protect from the transmission of malicious software, appropriate protection should be installed on the transfer systems, and be kept up to date.

5.7.4 File compression

File compression may be used to reduce the size of a data file, and thus reduce transfer and/or storage costs. Compression may be applied at the time of preparation or when electronic transfer is actioned. The type of compression is usually application dependent and may not be under the control of the user.

In a number of environments, the transfer channel will compress a file whilst it is in transit, this being transparent to the sender and recipient and implemented to give an improvement in the effective bandwidth of the transfer channel.

EXAMPLE

This type of ‘on the wire’ compression is most frequently required when slow, costly, transmission links are used. Whilst the sender and recipient may have no choice about this compression being used, they may be well aware of the effect of it.

An example of this is the, now widespread, use of videophones by reporters in the world’s trouble spots; the lower quality of the video and audio report is deemed an acceptable trade-off for the immediacy of the report.

Another, less obvious, but widespread application of such compression is found with all fax transmissions. In the first part of the transfer connection, before the fax image is transferred, the sending and receiving fax systems mutually agree the speed of transfer, the resolution of the scanned or otherwise rasterized image, and the compression mechanism for that image, which are supported by both sending and receiving fax systems; this is known as the negotiation phase.

File compression techniques should be used only in accordance with the policy document.

Authenticity should be protected when file compression techniques are implemented. Where it is important that no information is lost during the compression processes, lossless compression techniques should be used.

Details of the type of compression used (including the 'lossless'/'lossy' attribute) should be available to the recipient of a compressed data file, if they are required to access the information in that data file and confirm its authenticity.

Compression details may be stored within the data file, within its name (i.e. as the file extension) or as separate metadata. For example, a compression format frequently used for image files is known as tagged image file format (TIFF). In this format, the compression method is automatically stored within the file.

Where techniques that are inherently prone to data loss ('lossy') are used, they should be reviewed for acceptability.

EXAMPLE

Many electronically transferred transactions involve lossy compression. The recipient may be unaware of this; the sender has probably considered it as a key part of the underlying cost model for the transaction.

Most music downloaded from the internet is highly compressed in MP3 or advanced audio coding (AAC) format, giving approximately six or seven times more music than an equivalent CD.

Similarly, moving and still images delivered to low memory mobile devices (videophones, personal digital assistants [PDAs], etc.) will be using MPEG and JPEG compression at different compression rates compared with the same image when downloaded to a PC with its massive hard disk; MPEG (Moving Picture Experts Group, a joint ISO/IEC working group) has many related ISO/IEC Standards (under ISO/IEC JTC 1/SC29). MP3 is actually MPEG-1 Audio Layer III. JPEG (Joint Photographic Experts Group www.jpeg.org/jpeg/index.html) is covered in PD 0006:1995, and the ISO/IEC 10918 series. These compression standards for moving and still images respectively are lossy algorithms.

Lossy compression techniques may be acceptable when applied to continuous-tone material, or grey scale or coloured documents, where loss of information in the scanned image can be shown to be insignificant. Where text or line drawings are involved, however, such techniques may be unacceptable.

Where lossy compression is used, its attributes should be documented. This may be achieved by the use of typical transfer files, stored before and after compression.

KEY ISSUE

> Care should be taken when using lossy compression techniques, as significant information may be lost after decompression. Thus, the resultant information may differ from the original in information content, which may reduce its evidential weight.

5.7.5 File encryption

Where the confidentiality and integrity of information during electronic transfer is important, encryption techniques may be used. The information content of data files that are encrypted may not be viewed without the use of a decryption key and algorithm.

In some applications, 'unprotected' electronic transfers pose no threat or risk, where the viewing of information in a transferred file by another party may be acceptable. For such situations encryption may be unnecessary. Other cryptographic techniques, such as digital signatures, however, may be useful in protecting the integrity of the electronic document.

COMMENT – Digital signatures

A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and the integrity of the data to which it is applied can be verified. The algorithm used by the digital signature provides the capability to generate and verify signatures. Signature generation systems make use of a Private Key to generate a digital signature. Signature verification makes use of a Public Key which corresponds to, but is not the same as, the Private Key. Each user possesses a Private and Public Key pair. The Public Key need not be protected; it is normally held within the user's digital certificate which is included as a part of the signature. The digital certificate itself is normally signed by a trusted Certification Authority who has checked that the user's identity claims are backed up by sufficient evidence of identity (however, it is not uncommon for a user to self-sign a digital certificate in which case there is no third-party corroboration that the user is who they claim to be). Private Keys are never shared. Anyone can verify the signature of a user by employing that user's Public Key. Signature generation can be performed only by the possessor of the user's Private Key.

A hash function is used in the signature generation process to obtain a condensed version of the data to be sent, called a message digest. The message digest is then used to generate the digital signature, which is sent to the intended verifier along with the signed data (the message). The verifier of the message and signature re-calculates the message digest and then by using the sender's Public Key verifies both sender and message by comparison with the digital signature (which was created with the matching Private Key). The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data.

The policy document should detail levels of confidentiality required during transfer, for each document type.

COMMENT – Encryption

In some circumstances, any requirement for confidentiality may apply only when the data file is in the process of being transferred. In this case, encryption of the transfer channel as opposed to the data file may be acceptable. With 'channel' encryption, the connection 'pipe' is encrypted along with everything passing over it (and hence stopping anyone eavesdropping), but the contents are 'unprotected' to the communicating parties.

Where 'channel' encryption by itself is insufficient, data file encryption may be appropriate (not necessarily in isolation as an unencrypted data file may be transferred using an encrypted channel).

Typically, data file encryption will be necessary where the confidentiality of the data file is required within the sending or receiving system, for example, where only specific individuals are authorized to access the information in unencrypted form.

EXAMPLE

Many secure email services utilize S/MIME (Secure/Multipurpose Internet Mail Extensions), which provides a consistent way to send and receive secure MIME data (see IETF's RFC 3851). On the basis of the widely adopted internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications:

- authentication;
- message integrity and non-repudiation of origin (using digital signatures);
- data confidentiality (using encryption).

S/MIME can be used to add cryptographic security services to email that is sent, and to interpret cryptographic security services in received email. However, S/MIME is not restricted to mail; it can be used with any transport mechanism that carries MIME data, such as HTTP. As such, S/MIME takes advantage of the object-based features of MIME and allows secure messages to be exchanged in mixed transport systems.

A note of caution: to enable the internet mail infrastructure to route confidential messages that include S/MIME there are parts of the message that cannot be encrypted, for instance, the recipient and sender details. If the fact that these components are 'in clear' is a security risk then the use of an encrypted channel (using SSL or TLS) should be considered.

File encryption techniques should be in accordance with the legal requirements of the sender and receiver's jurisdictions, and of any other jurisdiction that the data file passes through (see 2.2.2.8).

File encryption techniques should be such that information is not lost during the encryption/decryption processes.

Details of the type of encryption used, and the relevant decryption keys should be available to the recipient if he or she is required to access the information in the data file.

Where encryption techniques are used, encryption and decryption keys should be stored securely, and should be available only to those authorized to use them.

COMMENT – Disclosure legislation

Legislation may exist mandating, under certain circumstances, disclosure of message content.

An example of this in England and Wales is the Regulation of Investigatory Powers Act 2000 (RIPA), which 'introduces a power to enable properly authorised persons (such as members of the law enforcement, security and intelligence agencies) to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information which they lawfully hold, or are likely to, in an intelligible form' (Explanatory Notes referring to section 49 of the Act). Furthermore, the Act also covers the disclosure of encryption keys used when messages are sent in encrypted form.

The disclosure of the encrypted message and the keys may be a necessity to establish that the 'intelligible form' disclosed was, in fact, the actual encrypted message transmitted.

Procedures for the management and allocation of encryption and decryption keys should be documented. These procedures should include key revocation, key recovery and key escrow processes where appropriate. These procedures are particularly important to cover the situation where the person who was responsible for their management is no longer employed within the organization.

Some countries have laws covering the use of encrypted data files within their jurisdictions. Such requirements should be reviewed and are to be complied with.

Care needs to be exercised where encryption technology is used for the maintenance of the integrity of an electronic document, to ensure that no specific confidentiality-related legislation compliance is compromised.

EXAMPLE

XML is a major enabler of what the internet and web services require in order to continue growing and developing as an environment for trustworthy electronic transactions. A lot of work remains to be done on security-related issues before the full capabilities of XML languages are realized. At present, the most important sets of developing specifications in the area of XML-related security are:

- XML encryption (www.w3.org/TR/xmlenc-core1/), XML digital signatures (www.w3.org/TR/xmldsig-core1/, also see ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES);
- XML Access Control Language or Extensible Access Control Markup Language (XACML), an OASIS Standard (http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf);
- SAML (Security Assertions Markup Language), an OASIS Standard (http://saml.xml.org/saml-specifications); and
- XML Key Management Specification – Version 2.0 (XKMS), (www.w3.org/TR/2005/REC-xkms2-20050628/).

Encrypting a complete XML document, testing its integrity and confirming the authenticity of its sender is a straightforward process. But it is becoming increasingly necessary to use these functions on specific parts of documents rather than the complete XML document, to encrypt and authenticate in arbitrary sequences, and to involve different users or originators.

This may mean, for example, that parts of an XML document are ‘in clear’ whilst those parts that contain personal data are encrypted.

KEY ISSUE

> File encryption may be used to increase the security on a data file, by reducing the risk of a third-party being able to access the information.

5.7.6 Sender and recipient identity

Information may need to be added to electronic information prior to transfer in order to enable the recipient to identify and verify who (individual and/or organization, process, application, system, device) is the sender of the data file; this is covered in more detail in BIP 0008-3. Similar identity considerations apply to the identity of the recipient.

KEY ISSUE

> Details of identity information used should be available to the recipient if he or she is required to verify the identity of the sender of the data file.

5.7.7 Multiple files

Where multiple files are being transferred, it may be appropriate to use sequence numbers within file names. These numbers are then used as a completeness check after receipt.

KEY ISSUE

> File sequence numbers may be used as part of the integrity confirmation information used where multiple files are transferred.

5.7.8 Integrity checks

The processes used for ensuring the integrity of the transferred information during the 'send' operation should be documented.

Where the transfer system is inherently lossless, checksums may be employed. They should be applied to the electronic document as part of the transfer system.

A checksum may be computed to include the date/time sent. Should any of the information including the date/time sent be changed (either accidentally or on purpose) on the received information, the checksum of the new information will be different from the sender's copy of the information. By automatically comparing the checksums of the sent and received copies of the information, a mismatch will indicate that information integrity has been compromised. Should this situation occur, the fact should be highlighted and re-transmission processes should be invoked.

EXAMPLE

Whilst from an evidential perspective it would be preferable for both the sender and the recipient to be able to present an identical electronic message, this is not always possible.

For example, an email collects metadata during its journey across the internet (although this may not be seen by the recipient); the email content may also have changed with the addition of a confirmation that it has been scanned for the absence of viruses by a third-party service provider contracted to the sender and/or the recipient.

Care should also be taken because an email can be displayed very differently when rendered by different email clients.

Cryptographic checksums (MACs) or digital signatures can provide additional strength for this control.

Where cryptographic techniques are employed for confirmation of integrity or identity, it is important that cryptographic keys are managed appropriately and not compromised. The actions to be taken and reporting to be followed in the event of actual or suspected compromise should be documented.

This process is frequently referred to as key management. As the entire digital signature and encryption operations are dependent upon the security of the keys, there should be rigorous processes in place to manage them.

Clearly, in the area of managing keys, roles and responsibilities should be defined. Typically, there should be segregation of roles. The staff involved in any aspect of key management should not be those who run the business from day to day, or have access to development systems or production systems.

In many organizations, all staff apart from those involved are obliged to leave the room when keys are being changed.

Sometimes, as in MACs, there is a requirement for secret keys to be sent to each participant for authentication of transmitted data. In this case, the keys themselves should be encrypted or transferred outside the normal transfer system.

EXAMPLE

If a secret key used for a MAC is compromised and known to a third-party, that third-party could modify the message and the recipient would be unaware of the changes. The recipient would also be unaware that the data file did not actually come from the expected sender because the MAC itself is genuine.

KEY ISSUE

> Methods for managing cryptographic keys used for checking the integrity of electronic transfer should be documented. This should include actions to be taken in the event of compromise.

COMMENT – Cryptographic keys

The two components required to encrypt data are an algorithm and a key. The algorithm is widely known but the decryption key is kept secret.

In a symmetric cryptosystem, the same key is used for encryption and decryption; therefore this key should not be used.

In an asymmetric cryptosystem, however, the key used for decryption is different from the key used for encryption; these are known as key pairs. Encryption is performed with the Public Key of the recipient and decryption with the recipient's Private Key; the Private Key should not be disclosed. In the majority of asymmetric cryptographic implementations, to reduce processing overheads, a symmetric encryption/decryption key is transferred using asymmetric encryption rather than the payload and the payload is encrypted/decrypted with that, securely transferred, symmetric key.

NOTE: for digital signature purposes, the signing process uses the signer's Private Key, and the signature is checked with the corresponding Public Key.

Where a certification authority is used, it is the Public Key that is certified, not the Private Key.

Keys should, whenever possible, be distributed by electronic means, enciphered under previously established higher level keys. There comes a point, of course, when no higher level key exists, and it is then necessary to establish the key manually.

A common way of doing this is to split the key into several parts (components) and entrust the parts to two people to reduce the risk of compromise. The two people put in half a key each, each going into a secure room alone to enter his or her part. That ensures no single person can ever normally know the key (other than where collusion is occurring).

It is important that none of the key parts contains enough information to reveal anything about the key itself.

A problem frequently occurs when it is necessary to re-enter a key from its components in this way. This is always an emergency situation, and it is often the case that one of the key component holders cannot be found. For this reason, sometimes the key components are distributed among three key holders in such a way that only two of them need to be present.

For example, if there are three key parts (P1, P2, P3) and three key holders (W1, W2, W3) then W1 could have (P1, P2), W2 could have (P2, P3) and W3 could have (P3, P1).

In this arrangement, any two of the three key holders would be sufficient. In many systems, the components are held on smart cards.

Where the transfer system is inherently prone to data loss (lossy), such as many real-time voice systems (where the human ear is better able to cope with slight gaps than data delivered fully, but out of natural sequence), alternative approaches to integrity are likely to be adopted. Whilst it might be possible to apply a checksum to the electronic transfer prior to storing or archiving, it cannot be applied 'on the wire' as what was sent and what was received may be different bit streams.

In these cases, it is important that the transfers are recorded accurately and retained and that the amount of 'data loss' can be shown to be within demonstrable and previously sampled limits that meet the defined acceptance criteria.

Transfer systems should report whether 'data loss' exceeds predefined thresholds, and appropriate predefined processes should be invoked.

KEY ISSUE

> Methods for checking the integrity of sent electronic transfers should be documented. This should include both lossless and lossy transfer systems.

5.7.9 Data file format exchange

Metadata may need to be added to electronic information prior to transfer in order to ensure that the recipient can determine the electronic format of the information content. Details of the format used should be available to the recipient if he or she is required to access the information in the data file.

The sender should ascertain the willingness of the recipient to accept a specific data file format. If the recipient indicates that he or she is unwilling to accept a specific data file format, the sender should select an appropriate, agreed alternative.

COMMENT –XML

XML is a simple, very flexible text format derived from Standard Generalized Markup Language (SGML) (BS 6868:1987 (EN 28879:1990, ISO 8879:1986). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the web and elsewhere. The specification of XML is controlled by the World Wide Web Consortium (W3C).

XML schemas express shared vocabularies and allow machines to carry out rules made by people. They provide a means for defining the structure, content and semantics of XML documents.

KEY ISSUE

> The acceptance of an agreed format for data file exchange should be documented.

5.7.10 Technology considerations

5.7.10.1 General

It is important to utilize reliable and trustworthy technology to facilitate electronic transfers. 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 at some time in the future. This demonstration may need to encompass both the technology itself and the methods by which it was configured and used.

Thus, implementers of electronic transfer systems need to ensure that they have been designed in accordance with the recommendations of the Code. This chapter contains details of processes that need to be implemented, enabling the defined procedures to be applied.

5.7.10.2 Transfer systems

There are many types of electronic transfer system, for example:

- email systems;
- short messaging systems (SMS);
- instant messaging (IM) and other peer-to-peer (P2P) 'presence'-based systems;
- fax systems;
- collaboration systems;
- point-to-point organizational systems;
- internal network systems;
- archiving systems;
- database extract, transform, load (ETL); and
- enterprise service bus (ESB).

Each of these has its own facilities and functionality. Relevant information is needed regarding the operation of all systems used for electronic transfer. Delivery and/or receipt may be at the organization, at specific premises or locations, within the system, or direct to and/or from the users, or any combination.

For each system, the following issues need to be addressed:

- internal organizational networks, either as a means of delivery to users connected to it or as a means of managing call charges, should be included in the transfer system;
- the use of public message switching services should be included;
- the use of synchronous or asynchronous messaging should be included.

The significance of any potential time delay in a document reaching the intended recipient should be documented. Such delays can be caused by:

- message switching and prioritization;
- network congestion;
- unavailability of a component or service in the message path; and
- message collection.

Similar delays can be caused where internet browser, internal email or other similar delivery systems are used. Integrity control, and confirmation of delivery and/or receipt systems should be included.

EXAMPLE

Although a fax-to-fax machine transfer may appear to be immediate there may be a considerable delay before it is received by the intended party, due to memory caching and/or paper handling procedures. Additional delays in fax transmission can be as a result of the use of fax servers or internet fax.

COMMENT – P2P file sharing

It was reported in early 2005 that the first malicious software or 'malware' (see 5.7.3) exploiting this vulnerability had been detected. Using P2P networks like Kazaa and eMule the malware uses features of Microsoft Digital Rights Management (DRM) (included in a wide range of its standard software) to create a secure channel whereby inappropriate or damaging software can be loaded, unnoticed by perimeter defences. These 'stealth mode' malware Trojan horses leverage the feature in the DRM software whereby if a copyright licence is not available on the user's system, a secure link is created to download a licence; in the case of the Trojan horse, the download is not a licence but a damaging payload.

Even if not compromising security, organizations should be careful about allowing users to make use of public IM or P2P file downloading systems. A survey in late 2004 indicated that of the Gnutella P2P traffic on the internet, 47 per cent related to pornography and 97 per cent infringed copyright. If this is through the organization's system, the organization may have unwittingly become responsible under the terms of vicarious liability.

5.8 Identity authentication

There should be documented processes that identify the senders and recipients of transferred documents. More details of these processes can be found in BIP 0008-3.

Where electronic transfer headers and/or confirmation of receipt fields are used, they should contain details of the person/application and/or the organization that sent the document.

Where an organization is involved in the sending and/or receiving of an electronic transfer, the identity of the organization should be included.

NOTE: This in itself does not prove the source of the document.

If passwords, PINs, biometrics and/or certified digital signatures are used, singularly or in combination, this will generally enhance the certainty that the sender/recipient is who he or she purports to be (see BIP 0008-3).

The issuance of keys and certificates will also provide supporting evidence of sender/recipient identity (see BIP 0008-3).

Where network information is provided by the electronic transfer system, this should be retained (e.g. calling line identification (CLI), URL). Care should be taken as to the value of this information, as it may be limited where such information has not been disclosed or when forwarding and relaying is involved.

KEY ISSUE

> See BIP 0008-3 for details of identity authentication.

5.9 Sender and recipient authentication

Sender and recipient authentication can be achieved in a number of ways, each of which may be of value to both parties. Techniques used may vary depending upon the information type being transferred. This is covered in more detail in BIP 0008-3.

Typical techniques include:

- sender or recipient identification trusted;
- sender or recipient identification guaranteed;
- sender or recipient identification verified by third-party;
- electronic information re-transfer to sender and confirmation received (possibly using alternative transfer methods); and
- electronic information stored or notarized by a TTP.

Techniques used for sender and recipient authentication should be documented.

Proving the recipient identity may in certain circumstances be unimportant. Frequently, electronic transfer confirmation of identity of an organization rather than of an individual will suffice to meet user requirements.

KEY ISSUE

> See BIP 0008-3 for more details of sender/recipient authentication methodology.

5.10 Identification of information

For subsequent distinguishing recognition purposes, each transferred data file should be allocated an unambiguous identifier by the sending system. This identifier should be transferred with the information.

Identifiers should be specific to the sending organization and consideration should be given to the risks inherent in an identifier not being unique.

Identifiers should be allocated such that should a dispute arise concerning transfer timing, prior and subsequent electronic transfer timings can be used in support as necessary.

The sender, recipient and subject of the data file should be clearly identified and this information should be transferred with the data file.

The processes whereby additional metadata are added automatically and/or manually to an electronic transfer should be documented. This additional metadata may (for example) be additional indexing information or version numbering, which will aid subsequent storage and retrieval of the electronic transfer.

DEFINITIONS

Metadata are data about data or, more fully, a description of the content and form of any resource. Examples include a shopping catalogue, describing the price, size, colour, brand and features of the items for sale, or the ‘properties’ section of an electronic file, giving the size, format, date created, creator and title of the file. Metadata can be added to, or attached to, a web page, file or database, or any other information resource. Metadata can be machine readable, giving software applications the data they need to interpret the information held on a file, or it can be designed more for human interaction, listing the creator, title, subject and other data needed to find or manage the resource.

KEY ISSUE

> Methods for the unique identification of transferred information should be implemented.

5.11 Transfer

5.11.1 Systems

Several transfer systems may be used, which may vary in terms of their quality of service, and which may or may not include the ability to detect and repair data file transmission errors automatically. Procedures used to determine which transfer system to use for each transfer document 'type' should be documented.

EXAMPLE

An example of differing service quality (but not of accuracy or of potential data loss) is where the immediacy of data file delivery is essential and a direct transmission will give this, but an indirect system (such as internet use) may not. The user will need to choose between what may be differentially charged alternatives.

Many voice and video protocols do not implement these processes. It may be more appropriate to lose a sub-second of a phone call than to insert it later in the audio stream out of sequence (the human ear is very good at accommodating lost data, within limits). This type of transfer is thus lossy.

COMMENT

As discussed previously, some compression algorithms are inherently lossy (e.g. JPEG, MPEG and MP3); it is also common for transfers themselves to be lossy.

Voice over Internet Protocol (VoIP), webcasts, videophones, video surveillance and telemedicine are all examples that involve transfers that have to cope with data loss. Typically, such data loss is caused by network congestion, unplanned or unexpected bandwidth constraints and transmission packets arriving out of sequence with the recipient.

In all these cases the received transaction will differ from that sent.

Lossy methods should be utilized only if documented quality targets can be demonstrated to be met under anticipated and actual operational conditions. Prior to the use of lossy transfer methods, a review and sampling of any impact should be conducted.

The amount of 'loss' can be very significantly affected by loading factors that may be uncontrollable by the parties at either end of the transfer link.

Where electronic transfer systems require manual intervention to initiate a transfer, procedures used should be documented.

KEY ISSUES

> Transfer systems should be appropriate to the information transfer requirements.

> Lossy compression should only be used where it is appropriate to do so.

5.11.2 Interim or temporary information storage

The processes whereby a sent or received data file, and confirmation of sending and receipt, is written to storage should be documented.

The controls described in BIP 0008-1 should be implemented to facilitate legally admissible storage. Where indexing processes are automated, processes used on receipt of an electronic file should be documented. Such processes should ensure that information include and/or have sufficient indexing information to enable effective subsequent retrieval.

KEY ISSUE

> Details of any temporary storage processes should be documented.

5.12 Receipt of transfer

5.12.1 General

Where electronic transfer systems require procedures to be carried out on receipt of a transfer, these procedures should be documented.

Where multiple techniques are employed, particular attention should be paid to ensure that the appropriate technique is used.

5.12.2 Malicious software

To protect from receipt of malicious software (e.g. viruses, macro viruses, worms and Trojan horses) or unsolicited messages (e.g. spam), appropriate protection software should be installed and kept up to date.

COMMENT – Malware

The 2013 Information Security Breaches Survey indicated that 59 per cent of large organizations were infected by viruses or malicious software. Virus infections continue to be among the more costly breaches to deal with. Despite making up only 2 per cent of the number of security breaches, virus infections contributed 14 per cent of the worst breaches of the preceding year. Virus infections were particularly significant in small businesses, where they contribute a sixth of the total breaches (up significantly on 2012) and a third of the worst ones.
www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report

Prevention is always better than cure. The cost of recovering from malware is frequently measured in thousands of pounds, which is not surprising when so many PCs in an organization get infected.

Malware is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server or computer network, for example, virus, spyware, etc.

In addition to malware there is spam (unsolicited commercial messages sent via email) and spim (unsolicited commercial messages sent via an IM system) to worry about. Volumes are massive and continue to grow in spite of the introduction of legislation in various parts of the world.

Procedures should be documented that reduce the possibility of computer viruses and other malicious software being included within information received by electronic transfer. Actions to be taken in the event of an electronic transfer demonstrating (or suspected of) the inclusion of such malicious software should be documented. This action may include notification back to the sender or receiver, refusal to accept or send the electronic transfer, quarantining, or disinfecting the electronic transfer prior to opening or forwarding.

KEY ISSUE

> Procedures for the protection from malicious software should be implemented.

5.12.3 Decompression

If data files are received in a lossless compressed format, they will need to be decompressed prior to presentation to the recipient.

If data files are transferred or stored in a lossless compressed format, decompression processes should be such that the integrity confirmation of received information is not compromised.

KEY ISSUE

> Where lossless compressed files are received, an appropriate decompression procedure should be documented.

5.12.4 Decryption

Where data files are received in an encrypted form, they may need to be decrypted prior to presentation to the recipient and/or storage.

Decryption processes should be such that the integrity confirmation of the transferred information is not compromised. The process should only be by/for the individuals or responsible role holders authorized.

KEY ISSUE

> Where encrypted files are received, an appropriate decryption procedure should be documented.

5.12.5 Sender identity

Where information has been added to electronic information prior to transfer, which enables the recipient to identify and verify who (individual and/or organization) is the sender of the data file, procedures for the handling of this information should be documented and in accordance with BIP 0008-3.

KEY ISSUE

> A procedure for adding sender identity information where appropriate should be documented.

5.12.6 Integrity verification

Some systems require that the integrity of a received file is checked before its information content is reviewed, forwarded or stored. Where this is the case, appropriate procedures should be documented.

Where an integrity checking system was used during the send operation (for example, the addition of a checksum), then the receiving system should confirm the integrity using appropriate technology.

Where the integrity cannot be checked by the receiving system, consideration should be given to re-transfer of the file back to the sender, for integrity verification.

In some applications, electronic files may need to be forwarded to the intended recipient and in some the recipient will collect or fetch a message from an intermediary. Forwarding systems should be such that the integrity of the transferred information is not compromised.

EXAMPLE

With IM and other P2P Session Initiation Protocol (SIP)-based systems, when completing a web form or when sending a fax, the sender and recipient are in direct contact. There is an end-to-end connection from sender to recipient (often passing through one or more intermediary systems). This differs from internet email, media downloads, file downloads, etc., where the recipient collects the message.

With internet email, Simple Mail Transfer Protocol (SMTP) enables the message to be forwarded across the internet in a number of asynchronous hops to reach, eventually, the recipient's post office. The recipient collects it from the post office using a standard, browser-based interface or with a mail client which is an application using a defined interface to the post office, either proprietary or an open standard such as Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP).

In some systems, file names, digital signatures and MACs are used to confirm the integrity of a received transfer. Where these systems are used, procedures for dealing with reported errors should be documented.

COMMENT – Message Authentication Codes (MACs)

Sometimes also called 'keyed hashes', MACs use cryptographic checksums and are an alternative to digital signatures. They can be used to verify the integrity and authenticity of an electronic transfer.

MACs are frequently used for file transfers where the transfer is between systems inside an organization and is frequently an automated process.

In this case, the sender of a transfer and the intended recipient share a secret key (unlike digital signatures where an asymmetric Public/Private Key pair is used). The sender uses the transfer and the key to compute the MAC, and sends the MAC along with the transfer. When the transfer is received, the recipient computes the MAC, and then checks to see if his or her MAC matches that sent with the message.

If it does, then the recipient knows that the transfer is from the other party that knows the secret key and that the transfer has not been changed since it was sent.

If a third-party does not have the secret key, then even though he or she may be able to modify the transfer, he or she cannot produce the matching MAC. Therefore, any alteration will be detectable.

MACs do not provide any secrecy; if confidentiality is required, the transfer should also be encrypted.

A useful source of information relating to MACs is the US Federal Information Processing Standards Publication (FIPS PUB) 198-1 July 2008
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf, The Keyed-Hash Message Authentication Code (HMAC) published by the National Institute of Standards and Technology (NIST) on 6 March 2002.

The specification in this standard is a generalization of IETF RFC 2104 (and update RFC 6151), HMAC: Keyed-Hashing for Message Authentication.

KEY ISSUES

> Procedures for the verification of the integrity of the received transfer should be documented.

> Where integrity checking systems were added to electronic transfers when they were sent, appropriate technologies should be used when they are received, to confirm integrity.

5.12.7 Confirmation of receipt

5.12.7.1 General

Upon receipt of electronic information, a confirmation of receipt should normally be sent to the sender. Receipt confirmation should be at least at the organizational level. Where appropriate, a personal receipt from the intended recipient should be sent. A time received identifier should be used, with the ability to distinguish between organization receipt and personal receipt, where appropriate.

This confirmation should include both details of the transfer document sent and an unambiguous confirmation of receipt, i.e.it should contain document details and recipient details.

EXAMPLE

The way in which a receipt is transferred from recipient to sender depends on the transfer methods used.

For example, this may be as an integral part of the transfer transaction itself, as in the case of IM or fax, where it is the final part of the transmission between the two systems.

In other examples, such as SMTP email or Simple Object Access Protocol (SOAP), the receipt is a separate, asynchronous, message that has sufficient metadata to allow the sending system to associate it with the original message.

The receipt confirmation may be electronically transferred information in its own right and, as such, it should be handled in accordance with the Code.

KEY ISSUE

> The processes used for receipt confirmation should be documented.

5.12.7.2 Use of SOAP

An electronic transfer confirming receipt of an electronic file (including the recipient identity) should be sent to the sender, or to a third-party, as proof of delivery if required. The format of confirmations of receipt should be agreed prior to their implementation.

COMMENT – Simple Object Access Protocol (SOAP)

SOAP is W3C's standard protocol for web services. Fundamentally, it provides a message exchange envelope for web service payloads. These payloads are frequently in the form of XML documents (which may themselves contain applications' data files).

SOAP provides the means by which the web service application-specific information may be conveyed in an extensible manner and supports the switching of SOAP messages by providing a full description of the required actions taken by a SOAP node on receiving a SOAP message. Most deployments of web services will require a SOAP envelope to transport the web service payload; they may or may not require the switching features of SOAP.

With a SOAP message it is possible to request a delivery receipt and the receiving system is obliged to honour the request. Therefore, the sending system can be assured of delivery (or will re-submit the message). In addition, the receiving system can detect duplicate messages and will discard the duplicates.

This capability is in direct contrast to SMTP email, where confirmed delivery is not supported.

Not everyone uses SOAP, a lot use Message-Oriented Middleware (MOM) for asynchronous messaging, frequently as a component of an Enterprise Service Bus (ESB) deployed for inter-system integration.

KEY ISSUE

> There should be procedures for any manual or automatic process that should be followed in order to verify the receipt of electronic transfers.

5.12.7.3 Confirmation data

The following information should be included with a transferred data file, to enable a confirmation of receipt to be transferred to the sender:

1. sender and recipient identity;
2. subject (and/or other information) of electronic transfer;
3. unambiguous electronic transfer identification;
4. sender time and date stamp;
5. sender's checksum on the file and associated metadata (may be a digital signature).

KEY ISSUE

> Listed above is the information to be sent with an electronic transfer (or included within it), so that a receipt confirmation message can be generated.

5.12.7.4 Receipt details

The following additional information should be returned to the sender and stored, by both the sender and the recipient, in such a way that it is linked with the transferred data file:

- sender and recipient identity;
- unambiguous electronic transfer identification (to enable the sender to match the receipt to the appropriate electronic transfer);
- sender's checksum on the file and associated metadata;
- received time and date stamp;
- checksum for the specific receipt covering the above data, including the checksum on the received electronic transfer (may be a digital signature).

KEY ISSUE

> Listed above is the information to be used to generate a receipt confirmation message.

5.12.8 Data file format exchange

The recipient should ensure that an electronic data file that has been received by transfer can be rendered, viewed, or otherwise accessed, in a form that retains the information content of the electronic data file.

EXAMPLE

Whilst from an evidential perspective it would be ideal for the sender and recipient of a particular electronic message to be able to retain identical messages, this is not always practical.

For example, an email collects metadata during its journey across the internet (although this may not be seen by the recipient); the email content may also have changed with the addition of a confirmation that it has been scanned for the absence of viruses by a third-party service provider contracted to the sender and/or the recipient. Care should also be taken because an email can look very different when viewed by different email clients.

Where a transfer cannot be rendered, consideration needs to be given to its acceptability. It may be necessary for the electronic transfer to be returned to the sender, with a request for rendering information.

EXAMPLE

There are three different ways in which communicating counterparties can establish their common capabilities to be able to transfer a message to ensure that it can be successfully interpreted:

1. prior, out of band, agreement;
2. capability negotiation as part of the transfer;
3. reference to a directory.

The first method is very simple. It could be as simple as the two parties to the transfer agreeing an acceptable data file format in a telephone conversation and agreeing to a separate telephone call to confirm that the message has been received and is accepted.

Typical of the second category is the fax negotiation phase. In the first part of the fax communications connection, before the fax image is transferred, the sending and receiving faxes mutually agree the speed of transfer, the resolution of the scanned or otherwise rasterized image, and the compression mechanism for that image that are supported by both sending and receiving fax systems.

Of the third type, an analogy is the use of the Yellow Pages. Web services that are available can be ‘discovered’; information about the available web services can be obtained from a ‘registry’, the standard for describing web services within the registry is Web Services Description Language (WSDL). WSDL provides the equivalent of a ‘tailor-made’ directory service for the dynamic discovery of web services; such dynamic discovery may be required to provide particular services to end users.

Only after acceptance by the recipient should a confirmation of receipt be sent. Acceptance covers the ability by the named recipient to view the information content of the data file. Care may need to be taken where intermediaries are involved, such as where someone views a data file on behalf of the intended recipient (see below).

Where the recipient of a transfer is not the intended final recipient, procedures should be implemented to ensure that the final recipient can render the electronic data file.

KEY ISSUE

> Procedures that ensure that the received electronic data files can be successfully rendered should be agreed prior to transmission.

5.13 Destruction

The procedures implemented by third-party service providers (including TTPs) when retained information is to be destroyed, deleted or expunged should be documented.

These procedures should be agreed with the organization to ensure that no information that should be retained is inadvertently destroyed, and also to ensure that all information that should be destroyed is not inadvertently retained.

EXAMPLE

Retention requirements are more fully covered in BIP 0008-1. There are particular cases where transfer transaction information has to be retained that is not defined by the business requirements of the organization or the TTP.

An example of this is in the requirement for the retention of data by communications service providers (CSPs) under the terms of the Anti-terrorism, Crime and Security Act 2001 and the subsequent disclosure of such data by CSPs under the terms of the RIPA.

The debate about who should fund this retention of data when they are not necessary to be kept for business purposes has been considerable.

KEY ISSUE

> Where destruction of retained information is required, procedures should be as covered in BIP 0008-1.

5.14 System maintenance

The electronic transfer system should be maintained by qualified and trained personnel to ensure that its performance does not deteriorate.

A maintenance log should be kept, detailing all preventive and corrective maintenance procedures completed.

Procedures for preventive maintenance should be documented. These procedures may be performed by system operators or by specialized service personnel.

KEY ISSUE

> Where maintenance (corrective or preventive) is required, it should be carried out by trained personnel.

5.15 Security and protection

5.15.1 Security procedures

The transfer systems should operate within the guidelines established in the information security policy. This requires the use of security controls appropriate to operational requirements. These controls and associated procedures should be documented.

The physical and operating environments for electronic transfer systems should be in accordance with the supplier's recommendations.

Encryption or signature techniques may be used to improve the security and integrity of electronic documents during transfer. Where such techniques are used, they should be in accordance with the recommendations of BIP 0008-3.

KEY ISSUE

> Security controls appropriate to the requirements of the information security policy should be implemented.

5.15.2 Access rights

5.15.2.1 General

There should be documentation available that details all levels of access available to the electronic transfer systems. These levels are typically as follows:

- system manager/administrator;
- user;
- system engineer.

The documentation should include access methods whereby only authorized staff can use or administer the system.

Where the transfer system utilizes encryption techniques to ensure that access to confidential data is restricted, access to keys should be controlled appropriately and documented.

It is not only individuals that have access rights; applications, services and devices can also be granted access to enter or amend data.

KEY ISSUE

> Access levels to transfer systems should be documented.

5.15.2.2 Access levels and third-parties

Where third-parties are given access to transfer systems, details of their access levels should be documented. These access levels may include:

- authorized client staff;
- authorized third-party service provider staff;
- system manager; and
- system engineer.

Where service provider staff have access to transfer systems, terms of the controls/checks applied to such staff should be agreed and documented. Controls/checks applied to such staff should be such as to ensure that they do not misrepresent or otherwise misuse the systems.

Where service provider staff have access to transfer systems, the service provider should verify that all such staff have entered into suitable non-disclosure and other confidentiality agreements.

Where transfers are with a third-party archiving organization, details of processes which ensure that access is allowed only to their own authorized information should be documented. This requires that there should be appropriate processes for the secure identification of individuals requiring access, and the management of authority levels for new/changed/deleted users.

KEY ISSUE

> Where third-parties are involved, access levels allocated to third-party staff should be controlled.

5.15.3 Business continuity planning

The unavailability of electronic transfer systems (even for a matter of minutes in some applications) can be a serious problem for organizations. Thus, procedures are required that can be implemented to control and minimize the impact of such a situation.

There is also the issue of recovery from failure during a particular transfer. It is important to ensure that transmission occurs once and only once, even when a transmission is interrupted by system failure (see also 5.7.8).

EXAMPLE

If a company's website is unavailable, even for a few minutes, valuable orders may be lost. Similarly, if the EDI service that is such an integral part of the 'just in time' supply chain is out of service, the order for parts might be delayed and production halted because of their shortfall.

These are very clear and direct results from a loss of service without adequate and effective business continuity plans being in place; the unavailability of a system such as email can be less obvious, but just as damaging for the business. Deprived of the main transfer channel that is email, how many knowledge workers quickly cease to work effectively? To get the picture, just look at the crowd that forms around the drinks machine if the email server is down!

Business continuity for electronic transfer systems is not managed simply by the availability of suitable alternative transfer facilities, as the unavailability of premises, staff or hardware needs to be included. Such procedures may involve the temporary use of additional or third-party resources.

In order to ensure that the integrity and availability of information being transferred electronically is not compromised during a loss of service, an agreed and approved business continuity plan should be implemented, covering the electronic transfer systems.

EXAMPLE

A key aspect to consider when developing and testing a business continuity plan is how long it takes to get a failed system back into full operation.

With an email service, it is not simply a case of getting the mail server back online, which may only take a matter of minutes. Without access to the contents of inboxes, sent items, shared and personal folders, contact lists, calendars and diaries, email users will, quite rightly, perceive that the email system is inadequate. Recovery of all these components may take hours longer than simply restarting the mail server.

Procedures should be established to include:

- major equipment, environmental or personnel failure;
- testing such procedures;
- maintaining such procedures;
- ensuring such procedures do not compromise the integrity of information during their implementation; and
- ensuring such procedures do not result in unwitting loss of electronically transferred documents.

EXAMPLE

Many electronic transfer systems include automated retry processes where successful transmission has not been completed.

With fax, there are standards governing how many times and how frequently a failed transmission may be retried automatically (but note that some low facility fax machines do not support this feature at all); these standards were originally set to restrict the number of 'annoyance' calls when a wrong number was entered into the sending fax.

With internet email, the SMTP process will automatically retry a transfer if, for example, the recipient's mail server is offline. In many cases the sender is totally unaware that this has happened. When repeated SMTP retries are required, the time before a subsequent retry is extended and may quickly become measured in days rather than minutes or hours.

KEY ISSUE

> Business continuity plans should include procedures that ensure the integrity of transferred information and, in particular, information in the process of being transferred at the time of failure.

5.16 Contracts

Where the exchange of electronic information is included in an agreement between two parties, any contract document should include clauses relevant to such exchange.

Where both parties agree to comply with the Code, the contract should include (or reference) all relevant documentation required. This should make the contract easier to apply in normal use, and in the event of a dispute. The key requirements identified in 2.2.2 should be included (or referenced) in the contract. The contract should be securely stored by the organization in compliance with BIP 0008-1.

KEY ISSUE

> Contracts with trading partners should include appropriate clauses to protect the organization during the electronic exchange of information.

5.17 Third-parties

5.17.1 General

Where a third-party service provider is used (for example, facilities management providers), there should be an appropriate contract in place. The contract should detail the services that are to be used. Such services should conform to the Code.

EXAMPLE

Contracts should include details on each of the following situations:

- information security measures;
- segregation from other clients' information;
- confidentiality measures;
- backup and recovery facilities;
- identity and authority checking procedures;
- service level agreements;
- availability of information, processes and procedures, audit trails and expert witnesses in the event of a dispute;
- liability;
- confirmation of compliance to appropriate codes of practice and standards;
- procedures for checking compliance.

Further details of recommendations for contract terms can be found in BIP 0008-1.

This contract should include agreements which will give the organization the capability to demonstrate compliance many years after the event, even if the third-party service provider has ceased to trade.

Where third-parties provide communications infrastructures (e.g. communications circuits without added value facilities), confirmation and underwriting of service levels concerning network availability and commitments to deliver data unaltered and unobserved need to be sought.

Where the third-party service provider subcontracts some or all of the provision, details of the procedures used by the subcontractor should be documented and responsibility for service provision clearly understood by all parties.

The organization should include in its agreement with the third-party service provider the rights to all relevant information held and procedures used in the event of:

- the third-party service provider ceasing to trade; and
- the organization, at the end of the agreement, deciding to use an alternative third-party service provider.

The controls over the exercise of these rights should be defined in the agreement with the third-party service provider.

Wherever service level agreements are part of the contractual provision of the transfer system service, reporting against these levels should be provided. This may need to be on an immediate basis rather than after the event.

Further details of the use and management of trusted third-parties can be found in BS ISO/IEC TR 14516.

KEY ISSUE

> When using third-parties to provide electronic transfer systems or services, appropriate contracts should be in place to manage the facilities used.

5.17.2 Cloud services

An important delivery method for externally provided services is leveraging internet technologies in what is called "the cloud". Every cloud service model involves the transfer of information from the using organization to the service provider(s) at some point in the service delivery. Therefore, it is important that information integrity is assured for any of these transfers and that transfer of information can be put into effect in the event that a service provider ceases operation or the using organization wishes to change service provider.

DEFINITION

The phrase 'in the cloud' is commonly used to refer to software, platforms, infrastructure, etc., that are sold 'as a service' and accessed by the user connected to the service provider's facilities and computing assets remotely through a network, commonly the internet.

The NIST, www.nist.gov/itl/cloud/index.cfm, publications regarding cloud computing identifies five essential characteristics of cloud computing:

- on-demand self-service;
- broad network access;
- resource pooling;
- rapid elasticity;
- measured service.

This use of the term 'as a service' has led to a number of service models, the first three featuring in the NIST publications (the list will grow in line with the imagination of marketing professionals):

- SaaS Software as a Service;
- IaaS Infrastructure as a Service;
- PaaS Platform as a Service;
- NaaS Network as a Service;
- DRaaS Disaster Recovery as a Service.

NIST have identified four deployment models:

- private cloud, operated solely for a single organization;
- public cloud, over a public network, such as the internet;
- community cloud, shared between a community of organizations with common concerns for security, jurisdiction, compliance, etc.;
- hybrid cloud, service provision using a combination of two or more clouds (private, community or public).

NOTE: Many cloud service provider's Terms of Service implicitly or explicitly acquire rights to the information on the service provider's infrastructure. This and the rights of the customer organization to this information at the termination of the business relationship, either planned or unplanned, should be considered.

KEY ISSUE

> Where the service provider operates in compliance with BS 10008, include in the service contract a statement making this compliance status a condition of contract, together with appropriate auditing requirements.

5.17.3 Audit trails

Users of third-party archives need to ensure that audit trail information as described in 4.5.3 is being created by the third-party, and is available to them in a timely and controlled manner.

KEY ISSUE

> Relevant personnel should have access to audit trail data commensurate with their role.

5.18 Time considerations

The processes implemented for the recording of electronic transfer date and time details should be documented. Consideration should be given to the format of this, especially when information is transferred across time zone boundaries.

Timings can be as follows:

- where documents are transferred in real time;
- where documents are stored and then transferred at a later time;
- where there is a difference between document receipt by an organization and by the person.

For 'store and forward' systems, or where receipt by a person is later than that by the organization, controls implemented to ensure that the document is not amended during its storage should be referenced.

Where the actual time that an event occurred is important, the use of trusted time from a third-party service provider should be considered (see 5.7.2).

Where available, and where time is important, processes for the recording of confirmed, Trusted Time stamps should be documented.

KEY ISSUE

> Where time is important, accurate time stamps are necessary.

5.19 Error handling processes

The processes used in error handling systems should be documented. They should be implemented to identify and correct received data errors.

Should an interruption occur during an electronic transfer, either the transfer should be cancelled and reinitiated, or a process should be implemented to provide a continuation transfer with clear referencing to the first electronic transfer where the service break occurred.

KEY ISSUE

> The handling of transmission errors should be documented.

6 Performance evaluation

6.1 Monitoring, measurement, analysis and evaluation

This section of the Code relates to Clause 8 of BS 10008, 'Performance evaluation'.

In order to be able to demonstrate the effectiveness of the management of transferred electronic information over time, the system used will need to be monitored and reviewed from time to time.

Thus, audits of the system should be undertaken at planned intervals. Such audits may:

- follow a regular pattern (such as on an annual basis);
- be based on significant changes to the system;
- be as a result of a major system failure; and/or
- be 'without warning'.

6.2 Internal audit

6.2.1 Audit requirements

The essential characteristics of an audit should be borne in mind when developing an audit plan for a procedure or system. The essential features of an audit are that it:

- has a clearly defined purpose;
- is based on clearly defined and measurable criteria;
- is planned and undertaken competently;
- reaches a fair and objective conclusion;
- is documented in each of these respects.

The results of an audit will be an audit opinion. Such an opinion should not mislead. The results should include a clear explanation of the purpose of the audit, identify the criteria on which the audit was based and describe the key features of the audit approach (e.g. sources of audit evidence, the extent of reliance on internal controls, use of sampling techniques and any significant assumptions). They should also describe the auditor's qualifications for undertaking the work.

KEY ISSUE

> Audits should be defined, planned and undertaken against agreed criteria to enable a suitable audit opinion to be reached.

6.2.2 Audit planning

The initial stage for the planning of an audit is to determine the purpose for the audit. Such a purpose may be to identify any nonconformance to procedures, or may be to confirm conformance to procedures.

Once the purpose has been established, the scope of the audit should be identified and recorded. Such a scope may encompass the whole organization, a particular part of the organization or a particular process being undertaken within the organization.

It may also be appropriate to define audit criteria. Such a definition will provide a benchmark against which to assess a process, with the objective of establishing the extent to which the audited process

complies with the criteria. Audit criteria take many forms, such as internal standards or procedures, specifications, codes of practice, industry sector standards, or contractual or statutory requirements.

Audit criteria may be internally or externally defined, and may be voluntarily, contractually or statutorily imposed. An audit may also aim to provide assurance that the criteria themselves adequately meet the requirements of the stakeholders in the audited process.

In practice, it is generally unnecessary to obtain a very high degree of assurance that audit criteria are met. It is typically sufficient for the audit to provide 'reasonable' assurance that the activity is free from 'material' error or nonconformance. However, this is not always the case. The evaluation and certification of systems for use in highly secure or safety critical systems is one example of a form of audit that aims to provide a high degree of assurance that audit criteria are met.

This level of assurance can only be provided on the basis of rigorous and time-consuming testing at commensurate cost.

An audit should be based on a quality plan, incorporating the relevant criteria, to provide a framework within which to work. This helps to ensure that all the activities that are necessary to meet the audit objectives take place in a logical sequence, are allocated to suitably skilled and experienced members of the audit team and are given appropriate weight in relation to their importance in forming an audit opinion. An audit plan also underpins discussions with the audited organization prior to the assignment, supports the agenda for the audit closure meeting and, together with the related audit reports and evidence, forms a permanent record of what has taken place.

KEY ISSUES

> Plan audits against an agreed purpose.

> The level of assurance obtained will depend upon good planning and adequate resource.

6.2.3 Audit procedures

Where a full system audit is undertaken, there should be procedures that review the following:

- that all applicable policies are being implemented in an appropriate manner;
- that established procedures are being followed;
- that appropriate technology has been implemented;
- that the technology is configured and maintained in accordance with requirements.

Where partial audits are undertaken, the procedures to be adopted should be such that the scope of the audit is followed.

There should be procedures for the recording of the audit results and of any appropriate analysis. Such results and analysis will lead to the audit opinion.

There should also be a procedure for the retention of evidence that an audit has taken place. It may be beneficial or even necessary, to provide external bodies with evidence that competently planned and conducted audits have taken place.

KEY ISSUES

> Audits may be undertaken of the whole or of part of a system.

> Retain evidence of audits.

6.2.4 Selection of auditors

Numerous individuals or bodies undertake audits. Each will have particular reasons for doing so and particular objectives to be met. For example:

- internal auditors provide top management with assurances that policies and procedures are being complied with;
- external auditors are used where an internal audit function is not available, or where an external opinion is required by the organization;
- certification bodies are used to certify against external standards, such as BS EN ISO 9000 and BS ISO/IEC 27001;
- industry regulators such as the Financial Conduct Authority (FCA) will verify compliance with regulatory requirements;
- government departments will assess and report on compliance with legal requirements, particularly in the accounts and taxes fields; and
- customers will monitor the activities of organizations with whom they trade.

Informal audits are also carried out routinely by line managers who review the procedures under their control, and assess these procedures for conformance to policy.

The important issue with the selection of auditors is that the audits are conducted in an objective manner, meet the audit requirements and produce impartial results.

KEY ISSUE

> Select the auditor with care, taking into consideration the required competency and independence.

6.3 Management review

6.3.1 General

In order to demonstrate that the system, including the related procedures, is continuing to provide the effective management of transferred information, regular management reviews should be undertaken. Further, these reviews should be undertaken whenever significant changes to procedures and/or technology are being planned and/or have been implemented.

KEY ISSUE

> Management reviews determine whether the objectives of the system are being met.

6.3.2 Basis for review

Management reviews should be based on:

- general and specific feedback from system users;
- results of the various audits (see 6.2);
- records of procedural reviews; and
- records of technology modifications.

6.3.3 Results

The management review should be used to assess whether compliance with BS 10008 is maintained. Where a risk is identified that compliance is or may be compromised, then a full review of compliance (see 6.3.4) should be undertaken.

KEY ISSUE

> Use the results of the management review to determine whether compliance with BS 10008 is maintained.

6.3.4 Demonstrating compliance

6.3.4.1 General

Information transfer systems should be audited on a regular basis to ensure that the provisions of the Code are being met and that the approved procedures are being adhered to. This audit should review audit trail data that are produced on a regular basis for evidence of ongoing, continuous compliance.

The compliance workbook, BIP 0009, may be used to enable a comprehensive assessment to be made of the user's system for conformity to BS 10008, and subsequently to the Code, and to help identify which parts of the Code are relevant to a system.

Compliance with the Code should be claimed only if all recommendations, as stated in the workbook, have been met, or justifications for any non-applicable recommendations documented. Compliance with the Code should be claimed via an authorized statement, examples of which are shown in 6.3.4.2.

The person identified in 2.3 as being responsible for maintaining compliance with the Code should review the results of each audit and document/implement a plan to address any non-compliances, which should be re-audited.

A record of compliance with the Code should be maintained, as part of the audit trail. This record should include details of which recommendations are not considered relevant, and justifications for these decisions.

Where compliance with previous editions of the Code has been claimed, copies of those editions should be retained as part of the compliance audit trail.

Where any change is made to the information transfer system, or to relevant procedures, which affects compliance with the Code, a new audit of compliance should be undertaken.

Auditing may be carried out by authorized and trained in-house staff or by suitable third-parties.

KEY ISSUES

> Use BIP 0009 to audit and document compliance with the Code.

> Re-audit on a regular basis, and during major system changes.

6.3.4.2 Statement of compliance

6.3.4.2.1 General

Compliance with the Code should be claimed using statements, which differ depending upon whether:

- the end user organization is claiming compliance;
- the system supplier is claiming that a system can be used in a compliant manner; and
- a third-party, acting as auditor, is confirming a compliance status.

Recommended text for use in compliance statements is given below. Alternative text may be used, but legal advice should be sought to ensure its suitability.

6.3.4.2.2 End user organizations

Individuals or organizations that conduct audits of their own information transfer systems may certify compliance via the following statement:

'[insert name of organization] confirms that the [insert name or other identification for the system] information transfer system is operated in compliance with BS 10008:2014.'

The statement should be signed by an officer of the organization, stating his or her position.

NOTE: The policy document should identify the individual or position within the organization authorized to sign statements of compliance with the Code (see Chapter 4).

6.3.4.2.3 System integrators and developers

Individuals or organizations that integrate/develop/supply information transfer systems may certify that their systems may be used in a compliant manner via the following statement:

'The [insert name or other identification for the system] information transfer system supplied by [insert name of integrator/developer/supplier] provides all facilities necessary for a user of this system for implementation in compliance with BS 10008:2014.'

The statement should be signed by an officer of the supplier organization, stating his or her position.

6.3.4.2.4 System auditors

Individuals or organizations that conduct audits of information transfer systems may certify compliance via the following statement:

'[insert name of auditing organization or individual] has assessed the [insert name or other identification for the system] information transfer system operated by [insert name of organization] for compliance with BS 10008:2014 and hereby certifies its compliance.'

The statement should be signed by an officer of the auditing organization, stating his or her position.

KEY ISSUE

> Claim compliance using an authorized statement.

7 Improvement

7.1 General

This section of the Code relates to Clause 10 of BS 10008, 'Improvement'.

It is important to improve procedures and systems wherever appropriate. Such improvements may be to ensure that an identified issue is resolved without compromise to the transferred information, and that the risk of a reappearance of the issue is minimized. The improvements may also relate to updated techniques and/or technology that will improve performance or reduce operational costs.

KEY ISSUE

> Ensure that procedures and systems are being maintained and improved by assessing the conclusions of audits.

7.2 Preventive and corrective actions

7.2.1 General

Any proposed improvement in procedures and/or technology should be assessed prior to its implementation to ensure that compliance with the information transfer and information security policies are not compromised.

Where major changes are implemented, an audit trail of the change management procedure should be produced and retained in line with the retention schedule. This audit should be completed as soon as possible after changes have been made.

7.2.2 Preventive

Preventive actions should be undertaken to reduce the risk of nonconformities in relation to compliance with the information transfer and information security policies.

The audit procedures identified in 6.2.3 should be followed at regular intervals to identify any nonconformity at an early stage.

Where a nonconformity is found, the cause of the nonconformity should be identified. An evaluation of the cause should then be completed, to identify the likelihood of the nonconformity reoccurring. Where the identified risk is significant, procedures and/or technology should be reviewed to identify ways of reducing this risk. Any identified actions from this review should be implemented.

The results of the review and details of the preventive actions taken should be documented and retained in accordance with the retention schedule.

KEY ISSUE

> Take preventive action to reduce the risk of nonconformities occurring.

7.2.3 Corrective

From time to time, issues will arise that will or may result in a nonconformity occurring. There may, for example, be an actual or a suspected security breach. In these instances, corrective action should be taken to:

- assess and document any compromise to the authenticity, integrity and/or availability of the information affected;
- identify and action procedures for recovery from any compromise (maybe by a restore from backup);
- reassess the stored information once recovery procedures have been implemented;
- document any residual issues found by the reassessment; and
- review the actions taken and identify (see 7.2.2) actions to be taken to prevent a reoccurrence of the issue.

KEY ISSUE

> Take corrective action to recover from nonconformities.

7.3 Continual improvement

7.3.1 General

There should be a mechanism for considering and acting on the findings of an audit. Although the auditor may recommend the general nature of any remedial action to correct problems uncovered by the audit, and may subsequently undertake further work to assess the extent to which remedial action has been successful, it is not the auditor's role to specify or impose particular solutions.

Organizations should review the results of all forms of audits (see 6.3) with an objective of continually improving the system. Such improvements can take many forms:

- system efficiency;
- system effectiveness;
- ease of operation;
- speed of operation;
- reduced risk of compromise to stored information;
- reduced risk of procedures not being followed.

KEY ISSUE

> Continual improvement should be an objective of the system.

7.3.2 Training

In order to be able to ensure that the procedures detailed in the procedures manual (see 4.5.2.3) are followed, staff need to be aware of them, and have the ability to follow them. This situation is frequently achieved by training, either by specific courses or during day-to-day working.

Training should be given to staff prior to them being given access to the appropriate parts of the system. Ongoing training should then be used to identify improvements within the system.

EXAMPLE

After specific training, the organization's group audit function took on the role of checking that procedures for the operation of all aspects of the information transfer system were being followed. Checks, including spot checks and scheduled reviews, were made at the same time as other audit checks were being made.

KEY ISSUE

> Training is needed to ensure that all staff who have access to the information transfer system adhere to agreed procedures.

Annex A Unstructured message considerations

A.1 General

Where organizations seek to maintain systems for the electronic transfer of unstructured messages in compliance with the Code, additional details should be included within the policy statement (see 2.2.2). Such systems are a significant form of inter-company messaging and include email, fax, SMS and IM systems.

The guidelines in this annex set out procedures that may be reviewed and, where appropriate, incorporated into the policy statement.

A.2 Policy objectives

The policy statement should cover the following key objectives:

- the creation of electronic message text;
- a policy regarding unsolicited messages (e.g. spam and spim);
- copyright and ownership;
- the storage and archiving of electronic messages;
- the receipt of electronic messages.

Typical contents of these sections are detailed below.

The organization should develop a policy appropriate to its own circumstances and should ensure that it is properly authorized, under appropriate change and version control, and demonstrably understood by and accepted by users as appropriate.

COMMENT

Some confusion could occur here over the term 'policy'. There may be multiple policies that may appear to overlap or conflict.

The organization should have a policy that is readily available to all staff, which makes their individual roles and responsibilities clear. This is critically important for unstructured transfers such as email, fax, SMS and IM. This may typically be part of the staff handbook or internet acceptable use policy.

The organization should have a policy for managing electronic transfers and this may, or may not, be readily available to all staff. This policy may refer to the staff handbook or internet acceptable use policy to avoid duplication (see 2.2.2).

KEY ISSUE

> The policy statement should be extended to cover unstructured message transfers, such as email, fax, SMS and IM.

A.3 Creation

Email, fax, SMS and IM are particularly informal forms of electronic transfer, and are classified as 'unstructured'. Typically, individual members of staff are able to include content and decide layout without corporate guidance. As such, and without special attention, these unstructured messages can result in transfer standards below those normally expected by the organization. In order to manage these issues, guidance is needed in how to create unstructured messages.

Thus, the policy statement should include points on:

- how to address messages, especially to individuals/organizations outside the organization;
- the importance of clear, single subject identification, as electronic messages are often dealt with based on this;
- writing standards (short, precise and to the point);
- spelling (often overlooked; spell-checkers should be used);
- circulation (often overdone, should be only on a need-to-know basis);
- open/closed copying (large lists of those copied may be unnecessary);
- illegal or potentially damaging electronic message content (e.g. libel, defamation, obsceneness and copyright breaching);
- attachments (ensuring they can be read by recipients);
- contracts (if contracts are concluded by electronic transfer, take care: some contracts need to be in paper form to be enforceable in certain jurisdictions. Take legal advice. If in doubt, send a paper copy for each party to sign); and
- electronic business. Arrangements for electronic business need to be carefully considered. As a baseline, the following need to be taken into account:
  - information retention requirements;
  - transfer requirements;
  - proof of identity; and
  - payment, or commitment to pay, for a specific product or service.

COMMENT

It is important to make people who have access to electronic message systems aware of the (lack of) confidentiality of messages sent in an unencrypted form.

It may be illegal to send some types of electronic message (e.g. those containing pornography). Other contents may have potentially damaging effects if disclosed to/intercepted by a third-party (e.g. those containing defamatory statements).

As a general rule, unencrypted electronic messages should only be sent if the content would also be appropriate for an open 'postcard' through conventional postal systems; with unencrypted messages there is no equivalent to the physical envelope that protects the content from inappropriate disclosure or from tampering. If an electronic message needs to be transferred in a confidential manner, then encryption is one technique that could be used.

In addition, the following issues should be addressed in the policy statement where relevant:

- personal passwords or alternative identity authentication (e.g. biometrics and identity tokens);
- encryption policy – define when encryption should be used and ensure the intended recipient can decrypt;
- lodging encryption keys or transactions with third-parties (see BIP 0008-3);
- international considerations – respect date, time of day and unit of measurement of the recipient and be aware of legal protection issues (e.g. trademarks);
- jargon – email, SMS and IM use their own jargon. Assess when and where it is acceptable;
- staff training policy – detail training provisions;
- procedures to be followed if an illegal or improper electronic transfer is found.

KEY ISSUE

> Rules regarding the creation of unstructured messages should be devised and implemented.

A.4 Spamming, filtering and viruses

The sending of unsolicited bulk messages by email (so-called 'spam'), SMS or IM ('spim') is illegal in certain jurisdictions. To guard against unlawful activities in this arena, appropriate policies should be devised and implemented.

Policy statements should include:

- adequate safeguards to ensure that unwanted, unsolicited messages do not reach workers;
- awareness and agreement by workers of actions to be taken on receipt of unsolicited messages;
- a requirement for procedures which ensure that illegal unsolicited messages are not generated; and
- a requirement for procedures to be actioned if unsolicited messages have been sent or may be received.

Filtering techniques are designed to stop unwanted incoming and/or outgoing messages by filtering their content. These techniques will, for example, identify foul or pornographic language and delete or quarantine such messages. These techniques can also, however, if too vigorously applied, filter out genuine electronic content.

The organization's workers and contractors should be aware of the use of these technologies and work within the rules applied.

Viruses are computer software that may cause major damage to any computing system that they come into contact with. They are often received through incoming messages (email is currently the major source of such malicious software, but it is spreading to other messaging forms like IM, and to mobile phones, PDAs and other such devices).

The organization's workers and contractors should be made aware of the danger from viruses and other malware received through electronic messages. They should be required to comply with the organization's policy for the detection and defence against message-borne viruses and other malware.

Virus and other malware control software will not automatically identify all viruses, as new ones are continually being created. It is thus important to ensure that such systems are regularly updated.

The organization's workers and contractors should:

- be aware of the risks from the various forms of spam and malware;
- take appropriate preventive action where necessary; and
- immediately report any suspected spam, virus or other malware.

KEY ISSUE

> Protection against the various forms of unsolicited messages and malware should be implemented and kept up to date.

A.5 Copyright and personal use

A.5.1 Policy

Workers have rights and responsibilities concerning electronic messaging and so does the organization. A policy should be developed in relation to these rights, to meet organizational needs. This policy should clearly define the rights of the organization and of the individual, especially in the area of the use of the organization's messaging resources for personal matters.

This policy should be carefully drafted and should be in accordance with general organizational policies with regard to workers, as too rigorous a policy may be unenforceable and may lead to worker unrest, whereas too lenient a policy may encourage abuse. The policy should be written in such a way that it is understood by all workers.

It may be appropriate to take legal advice when drawing up this policy.

In order to ensure implementation of the policy, compliance should be a part of the worker's contract of employment. When subcontractors and other third-parties use the organization's messaging facilities, an agreement relating to their use should be part of the related contract.

A.5.2 Copyright

Copyright of electronic messages typically resides with the sender of the message unless agreed otherwise. Most organizations may wish to place ownership under their own control. Thus, appropriate agreements on this issue need to be included in the worker's contract of employment, or other equivalent document.

A.5.3 Privacy

Privacy rights of the individual sender and recipient will vary from country to country. Within the UK, these are typically found in the Data Protection Act 1998 and the RIPA. Electronic messaging systems operating across national borders may give rise to additional privacy issues relating to the different countries involved.

In the absence of an explicitly accepted policy, users may have a legal right to assume that their transfers will remain private.

To meet corporate requirements, organizations will typically need to have rights of access to electronic transfers handled by their workers. To ensure that this is within their legal rights, they may need to gain explicit prior agreement to this from their workers and subcontractors.

A.5.4 Personal use

It may be appropriate to allow limited personal use of electronic messaging systems. Such rights and responsibilities should be defined by the inclusion of appropriate words in the worker's contract of employment.

Organizations should be aware that, if an worker with personal use of his or her electronic messaging system becomes the subject of an investigation (e.g. criminal or civil), the organization may be required to provide evidence of the worker's use of the system and may be responsible for the effects of its worker's actions.

A.5.5 Monitoring

With the ownership of copyright come related responsibilities. The organization should assess its risks in this area and formulate an appropriate message monitoring control policy.

At one extreme, companies may be legally required to monitor electronic messages, for example, to ensure that illegal messages are not created and sent. At the other extreme, regulations may preclude monitoring, for example, in the personal correspondence with the worker's trades union representative. For international messaging, the legal situation in each country may need to be reviewed. Finally, the type of businesses involved and risks being taken need to be put in the balance.

To manage these issues, organizations should have a clear, implemented policy for the monitoring of electronic messages.

To ensure that workers are able to understand the policy in detail, it should be drafted in simple terms, and training and/or other awareness methods should be available as and when required.

To avoid friction with workers in the development of such a policy, it may be appropriate to include them in the development of the policy, and encourage their contribution to creative ideas in the use of company messaging technology.

A.5.6 Breaches, procedures and penalties

The policy should set out the worker position should a breach occur, the procedures to be followed and penalties that may ensue. Typical penalties range from a simple 'ticking off' to dismissal. Such penalties should be included in the policy document, and should be applied irrespective of the worker's position within the organization.

KEY ISSUE

> Policies for the use of electronic messaging for personal purposes, including copyright and monitoring issues, should be included in the policy document.

A.6 Retention and destruction

Much electronic messaging activity is informal, and will not be required for long-term retention/record keeping/archiving purposes. Some messages, however, may by law be required to be kept for a minimum period.

To ensure the availability and integrity of retained messages, the retention should be under the terms of BIP 0008-1.

Where an organization has a corporate retention policy, electronic messages should be included within that policy. They should not be included as a specific, single 'document type'. A method of classifying individual messages and then allocating them an appropriate retention period should be the normal process.

EXAMPLE

Electronic message categorization may best be managed by enabling the worker to identify messages that need to be kept beyond a short retention period. Those for longer storage should then be copied to an electronic storage system outside the messaging system.

This process should be a 'mirror' of the related paper-based system. When a message on paper is received, it is either dealt with and stored 'on file', or it is dealt with and discarded immediately. An example of the first action is where an application form for a service is received. The second action could be appropriate for a notice of a meeting.

The following issues should be considered and, if necessary, risk assessments should be made before policies are implemented:

- normal retention periods for electronic messages may be relatively short (30–90 days);
- longer retention periods could possibly create higher risks for the organization;
- conversely, longer retention periods could lower risks by protecting the organization against claims that the content was inappropriate or defamatory – remember, however, that the sender or recipient who was once trusted may have a copy of the message and may now be an adversary'
- some electronic messages will need long-term retention/archiving for legal or regulatory purposes'
- these types of document/email need to be clearly identified, and staff need to be made aware of this. This applies to both sent and received electronic messages, which should be retained according to the policy;
- disclosure orders – be aware that authenticated copies of appropriate electronic messages may need to be disclosed in court (see BIP 0008-1 for details of authentication methods);
- deletion processes need to ensure that the original, together with all copies, backups and external copies (e.g. on laptops, mobile phones and PDAs) are deleted.

KEY ISSUE

> Corporate retention policies should be applied to electronic messaging systems. A policy of short retention periods for all messages may not meet legal requirements.

Electronic messages in the form of email, fax, SMS and/or IM lend themselves to rapid transfer. Senders typically expect an immediate reply. They assume that delivery has been achieved and that the message has been read, within a short time interval from their send time. This may not be the case, due to delays in transmission or the unavailability of the recipient to deal with the message. Messages may not be delivered, due to addressing errors, system failure or filtering mechanisms.

Some messaging systems include a 'proof of delivery' option, whereby the recipient is asked to confirm receipt. Whilst the receipt of such a confirmation message may be trustworthy, the absence of such a receipt may not be reliable evidence as to either delivery or non-delivery.

Policies for use in relation to received electronic messages should consider receipt from a customer service viewpoint, with typical issues to be covered including:

- the use of filtering systems to exclude unsolicited messages and malware from electronic transfers – over-filtering may, however, result in lost orders;
- the verification of the identity of the sender;
- the verification of receipt and/or reading;
- prompt and courteous replies (where needed);
- referring to the sender's subject or reference – develop policy on sending incoming electronic messages with replies, as appropriate;
- if necessary, forwarding to appropriate parties – if necessary, seek permission to forward. Note that copyright typically resides with the sender (author);

- a productivity policy – electronic messaging can be very time consuming;
- assessing the value of subject previewing and/or organizing set times for handling, to improve productivity; and
- considering the role of a gatekeeper to monitor/direct incoming electronic messages.

KEY ISSUE

> Policies on the handling of received messages should bear in mind the expectations of the sender.

Annex B – Example electronic transfer policy statement

This annex contains an example 'electronic transfer policy statement'. It can be used as a draft upon which an organization's policy can be based.

XYZABC Limited

ABC project

Policy document for compliance with the requirements of BS 10008:2014, *Specification: Evidential weight and legal admissibility of electronic information*.

Approved by:	
Name:	
Position:	
Date:	

1. Scope

This document covers the information transfer policies implemented within the XYZABC Limited electronic transfer systems. This policy conforms to the requirements of BS 10008:2014, *Specification: Evidential weight and legal admissibility of electronic information.*

The electronic transfer system consists of the following:

- HIJ electronic transfer system;
- KLM internet web service;
- PQR automated reporting system;
- XYZABC Limited email system;
- XYZABC Limited facsimile server system and stand-alone facsimile machines.

These electronic transfer systems are described in a system description manual (Ref: SD02). Procedures for the use of the systems are described in a procedures manual (Ref: PM02).

2. Information covered

Transferred information covered by this policy document relates to those messages used in relation to all aspects of electronic transfer for XYZABC Limited.

XYZABC Limited does not operate an information classification system, as all information is regarded as having the same security level.

3. File formats

All transferred information (messages, message metadata and message attachments) is transferred in formats agreed with the recipients.

4. Standards

All electronic information transfer within XYZABC Limited is transferred in compliance with BS 10008:2014 and BIP 0008-2 (2014), together with any referenced national and/or international standards.

All electronic information transfer within XYZABC Limited is stored in compliance with BS 10008:2014 and BIP 0008-1 (2014).

5. Data file and document transfer

5.1 General

The transfer policy has been agreed within XYZABC Limited to cover legal and operational requirements consistent with the status of being a public limited company.

All transfer systems used within XYZABC Limited are the property of XYZABC Limited and are provided to help meet the business aims and responsibilities of XYZABC Limited; staff, contractors and others using these systems have no expectation of privacy relating to their use of these transfer systems.

5.2 Structured

This section deals with electronic documents transferred with the:

- HIJ electronic transfer system;
- KLM internet web service; and
- PQR automated reporting system.

For each document type the following will be considered:

- data file formats;
- compression and encryption;
- pre-transmission processes;
- transfer channel to be used;
- post-transmission processes;
- integrity confirmation;
- confirmation of identity of sender/recipient;
- conformation of delivery/receipt;
- responsibility for message.

5.3 Unstructured

This section deals with transfer messages that are sent or received on an ad hoc basis. This includes person-to-person email and fax transfers.

NOTE: Email and fax transfers generated automatically from the PQR automated reporting system are included under the terms of the previous section.

Email and fax systems are provided to facilitate effective business transfers and may be used for limited personal use as defined in the staff handbook.

In all cases where a document has been sent or received, it will be retained and, at the appropriate time, destroyed in compliance with BS 10008:2014 and BIP 0008-1 (2014).

Unstructured messages by email and fax can be highly effective, if properly used, or highly damaging, if improperly used. Guidelines for proper use and sanctions that will be imposed for improper use are detailed in the internet acceptable use policy (Ref: IAUP02).

These guidelines include, but are not restricted to:

- the creation of messages;
- virus and other malware protection;
- unsolicited bulk messages;
- copyright, ownership and monitoring;
- receipt of and reply to messages;
- storage and retention of messages (in compliance with BIP 0008-1 (2014)); and
- personal use.

In addition, other criteria to be applied to specific message types includes but is not restricted to:

- when and how encryption is to be used;
- when and how message integrity is to be confirmed;
- when and how the identity of the sender and recipient are to be checked;
- whether proof of delivery is required; and
- what pre- and post-transmission checks should be performed.

Use of email systems other than those provided by XYZABC Limited is not allowed and any use of other email systems on XYZABC systems or premises is in breach of the terms detailed in the staff handbook that form part of the contract of employment.

Instant messaging, other than that of the restricted users of the KLM system, is not allowed and any use on XYZABC systems or premises is in breach of the terms detailed in the staff handbook that form part of the contract of employment.

6. Responsibilities

This policy document should be reviewed annually under the control of the company secretary. Where changes are agreed, they are to be implemented using the change control procedures (Ref: CC01).

This policy, and any revisions to it, should be approved by the Board of Directors of XYZABC Limited prior to implementation.

The maintenance of compliance with BS 10008:2014 is the responsibility of the Head of Internal Audit.

7. Legal advice sought

XYZABC Limited has sought and obtained agreement for this transfer policy.

8. Duty of care

XYZABC Limited has a duty to keep secure and accurate original documentation, or authentic copies of them. This is achieved by:

- implementing this policy document;
- implementing an information security policy;
- ensuring that only trained staff have access to the system;
- ensuring that acceptable quality control procedures are implemented; and
- ensuring that XYZABC Limited's legal advisers are consulted, and appropriate actions taken.

Annex C References

BSI publications

British Standards Institution, London. BSI Publications are available from Customer Services, Sales Department, 389 Chiswick High Road, London W4 4AL. Tel: 020-8996-9001; Fax: 020-8996-7001

Standards

BS 6868:1987 (EN 28879:1990, ISO 8879:1986), *Specification for Standard generalized markup language (SGML) for text and office systems* (ISO title: *Information Processing — Text and Office Systems — Standard Generalized Markup Language (SGML)*)

BS 10008:2014, *Evidential weight and legal admissibility of electronic information — Specification*

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

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

BS ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

BS ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

BS ISO/IEC TR 14516:2002, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*

ISO/IEC 10918 series, *Information technology — Digital compression and coding of continuous-tone still images*

Guidance documents

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*

BIP 0009 (2014), *Evidential weight and legal admissibility of electronic information — Compliance workbook for use with BS 10008*

PD 0006:1995, *Technical guide to JPEG — Digital compression of photographic images*

Other publications

ANSI X9.95:2012, Trusted Time Stamp Management and Security

Services Industry (rDSA), New York: American National Standards Institute (ANSI)

Signature Algorithm (ECDSA), New York: American National Standards Institute (ANSI)

ETSI TS 102 023 (2003), Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, Sophia-Antipolis: European Telecommunications Standards Institute (ETSI)

ETSI TS 101 903 XML V1.3.2 (2006-03), XML Advanced Electronic Signatures (XAdES), Sophia-Antipolis: European Telecommunications Standards Institute (ETSI)

Federal Information Processing Standards Publication (FIPS PUB) 180-2 (2002), Secure Hash Standard (SHS), Gaithersburg: National Institute of Standards and Technology (NIST). Available at: http://csrc.nist.gov/publications/PubsFIPS.html

Federal Information Processing Standards Publication (FIPS PUB) 198 (2002), The Keyed-Hash Message Authentication Code (HMAC), Gaithersburg: National Institute of Standards and Technology (NIST). Available at: http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

Anti-terrorism, Crime and Security Act 2001, London: The Stationery Office. Available at: www.legislation.gov.uk/ukpga/2001/24/contents

Regulation of Investigatory Powers Act 2000, London: The Stationery Office. Available at: www.legislation.gov.uk/ukpga/2000/23/contents

Data Protection Act 1998, London: The Stationery Office. Available at: www.legislation.gov.uk/ukpga/1998/29/contents

RFC 2104 (1997) HMAC: Keyed-Hashing for Message Authentication, Internet Engineering Task Force (IETF) See www.ietf.org/rfc/rfc2104.txt?number=2104

RFC 3161 (2001) Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), Internet Engineering Task Force (IETF). See www.ietf.org/rfc/rfc3161.txt?number=3161

RFC 3851 (2004) Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, Internet Engineering Task Force (IETF). See www.ietf.org/rfc/rfc3851.txt?number=3851

RFC 5816 (2010) ESSCertIDv2 Update for RFC 3161, Internet Engineering Task Force (IETF). See www.ietf.org/rfc/rfc5816.txt?number=5816

RFC 6151 (2011) Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms, Internet Engineering Task Force (IETF). See www.ietf.org/rfc/rfc6151.txt?number=6151

Evidential weight and legal admissibility of information transferred electronically

Code of practice for the implementation of BS 10008

Evidential weight and legal admissibility of information transferred electronically – Code of practice for the implementation of BS 10008 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.

Now in its fifth edition, the book provides a valuable framework and guidelines that identify key areas of good practice for the implementation and operation of electronic communications systems, whether or not any such information is ever required as evidence in the event of a dispute. 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.

This fifth edition is technically similar to the fourth edition, 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, and can be considered to be a guide to the implementation of the standard in relation to information transferred electronically.

This publication is the second part of BIP 0008. The other two parts are:
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.*

This book provides guidance on how your organization can:
- improve reliability of, and confidence in, communicated information;
- maximize the evidential weight which a court or other body may assign to presented information;
- provide confidence in inter-company trading;
- provide confidence to external inspectors (for example, regulators and auditors) that the organization's information and business communications practices are robust and reliable.

Peter Howes

Peter Howes is Director and Principal Consultant for Group 5 Training Limited and is a specialist in the practical issues of legal and regulatory compliance, governance, electronic communications and information security, with over 40 years' relevant experience in the business application of information systems. For the last 20 years, Peter has worked with BSI to develop the full range of evidential weight and legal admissibility publications and has delivered a wide range of workshops on evidential weight as well as email records management, email and the law, information security and the law with BSI.

Alan Shipman

Alan Shipman is Managing Director and Principal Consultant for Group 5 Training Limited. He has been involved in Document Imaging Standards for over 20 years, specializing in user aspects. Alan is Chairman of the BSI Document Imaging Applications committee, convenor of the ISO Document Imaging Quality sub-committee and a member of the UKAIIM Standards Committee. Alan has presented BSI Training Workshops on the practical implementation of BIP 0008, as well as speaking on the subject at events in the information management, archives and records management fields and also at industry specific events in educational, engineering, health care, financial, legal, local government and system supplier fields.

bsi.

BSI Group Headquarters
389 Chiswick High Road
London W4 4AL
www.bsigroup.com

BSI order ref: BIP 0008/2

The British Standards Institution is incorporated by Royal Charter

9 780580 856778