

Information security management systems — Specification with guidance for use

ICS 03.100.01; 35.020

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to BSI-DISC Committee BDD/2, Information security management, upon which the following bodies were represented:

@stake

Articsoft Ltd

Association of British Insurers

British Computer Society

British Telecommunications plc

British Security Industry Association

Department of Transport and Industry — Information Security Policy Group

EDS Ltd

Experian

Gamma Secure Systems Limited

GlaxoSmithKline plc

HMG Protective Security Authority

HSBC

I-Sec Ltd

Institute of Chartered Accountants in England and Wales

Institute of Internal Auditors — UK and Ireland

KPMG plc

Lloyds TSB

Logica UK Ltd

London Clearing House

Marks & Spencer plc

National Westminster Group

Nationwide Building Society

QinetiQ Ltd

Shell UK

Unilever

Wm. List & Co

XiSEC Consultants Ltd/AEXIS Security Consultants

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Policy and Strategy Committee and comes into effect on 5 September 2002

© BSI 5 September 2002

First published as Part 2
February 1998
Revised May 1999

The following BSI references relate to the work on this British Standard:
Committee reference BDD/2
Draft for comment 01/682010 DC

ISBN 0 580 40250 9

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
<hr/>	
0 Introduction	1
1 Scope	3
2 Normative references	3
3 Terms and definitions	3
4 Information security management system	5
5 Management responsibility	8
6 Management review of the ISMS	9
7 ISMS improvement	10
<hr/>	
Annex A (normative) Control objectives and controls	11
Annex B (informative) Guidance on use of the standard	22
Annex C (informative) Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002	28
Annex D (informative) Changes to internal numbering	30
<hr/>	
Bibliography	33
<hr/>	
Figure 1 — PDCA model applied to ISMS processes	2
<hr/>	
Table B.1 — OECD principles and the PDCA model	27
Table C.1 — Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002	28
Table D.1 — Relationship between internal numbering in different editions of BS 7799-2	30
<hr/>	

Foreword

This part of BS 7799 has been prepared by BDD/2, Information security management. It supersedes BS 7799-2:1999, which is obsolescent.

This new edition has been produced to harmonize it with other management system standards such as BS EN ISO 9001:2000 and BS EN ISO 14001:1996 to provide consistent and integrated implementation and operation of management systems. It also introduces a Plan-Do-Check-Act (PDCA) model as part of a management system approach to developing, implementing, and improving the effectiveness of an organization's information security management system.

The implementation of the PDCA model will also reflect the principles as set out in the OECD guidance (2002)¹⁾ governing the security of information systems and networks. In particular, this new edition gives a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

The control objectives and controls referred to in this edition are directly derived from and aligned with those listed in BS ISO/IEC 17799:2000. The list of control objectives and controls in this British Standard is not exhaustive and an organization might consider that additional control objectives and controls are necessary. Not all the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not in itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 33 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

¹⁾ OECD. *OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security*. Paris: OECD, July 2002. www.oecd.org

0 Introduction

0.1 General

This British Standard has been prepared for business managers and their staff to provide a model for setting up and managing an effective Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by business needs and objectives, resulting security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that simple situations require simple ISMS solutions.

This British Standard can be used by internal and external parties including certification bodies, to assess an organization's ability to meet its own requirements, as well as any customer or regulatory demands.

0.2 Process approach

This British Standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of an organization's ISMS.

An organization must identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs, can be considered to be a process. Often the output from one process directly forms the input to the following process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

A process approach encourages its users to emphasize the importance of:

- a) understanding business information security requirements and the need to establish policy and objectives for information security;
- b) implementing and operating controls in the context of managing an organization's overall business risk;
- c) monitoring and reviewing the performance and effectiveness of the ISMS;
- d) continual improvement based on objective measurement.

The model, known as the "Plan-Do-Check-Act" (PDCA) model, can be applied to all ISMS processes, as adopted in this standard. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes (i.e. managed information security) that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses 4, 5, 6 and 7.

EXAMPLE 1

A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.

EXAMPLE 2

An expectation might be that if a serious incident occurs — perhaps hacking of an organization's eBusiness web site — there should be people with sufficient training in appropriate procedures to minimize the impact.

NOTE The term "procedure" is, by convention, used in information security to mean a "process" that is carried out by people as opposed to a computer or other electronic means.

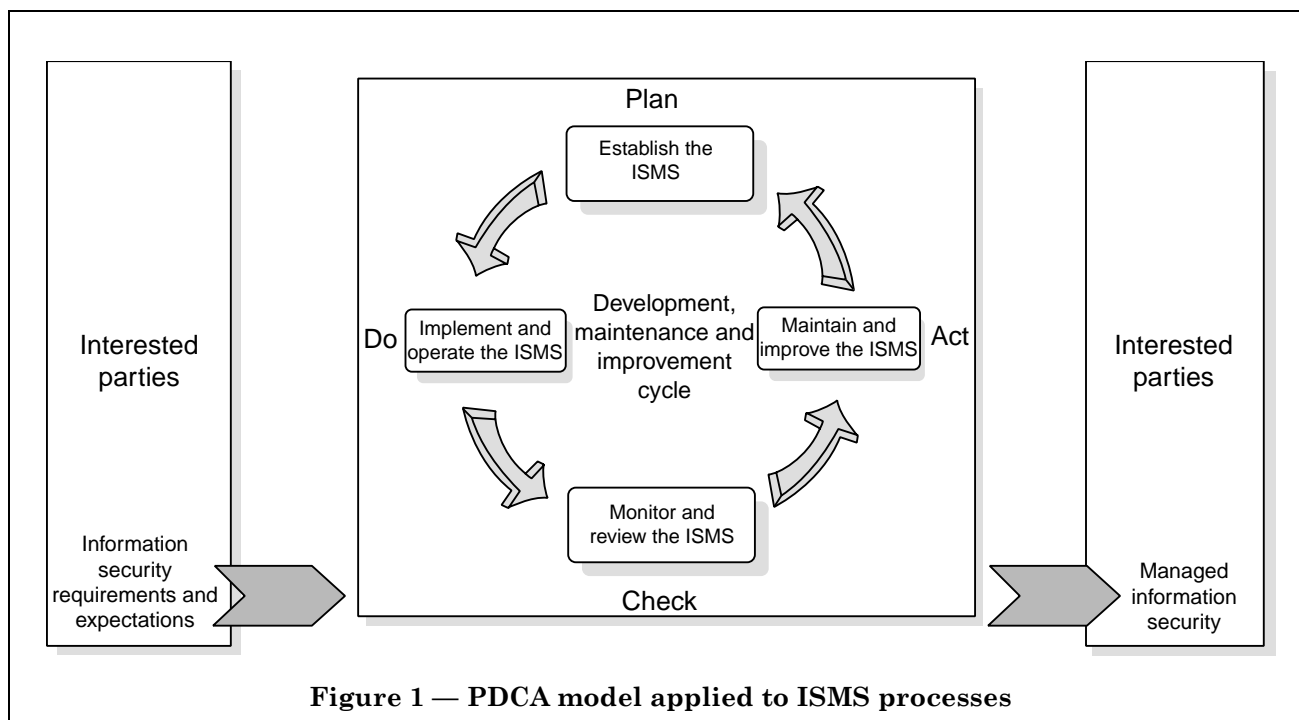


Figure 1 — PDCA model applied to ISMS processes

Plan (establish the ISMS)

Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

Do (implement and operate the ISMS)

Implement and operate the security policy, controls, processes and procedures.

Check (monitor and review the ISMS)

Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.

Act (maintain and improve the ISMS)

Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS.

0.3 Compatibility with other management systems

This standard is aligned with BS EN ISO 9001:2000 and BS EN ISO 14001:1996 in order to support consistent and integrated implementation and operation with related management standards.

Table C.1 illustrates the relationship between the clauses of this British Standard, BS EN ISO 9001:2000 and BS EN ISO 14001:1996.

This British Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.

1 Scope

1.1 General

This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof (see Annex B which provides informative guidance on the use of this standard).

The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.

1.2 Application

The requirements set out in this British Standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature of business. Where any requirement(s) of this standard cannot be applied due to the nature of an organization and its business, the requirement can be considered for exclusion.

Where exclusions are made, claims of conformity to this standard are not acceptable unless such exclusions do not affect the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable regulatory requirements. Any exclusions of controls found to be necessary to satisfy the risk acceptance criteria need to be justified and evidence needs to be provided that the associated risks have been properly accepted by accountable people. Excluding any of the requirements specified in Clauses 4, 5, 6 and 7 is not acceptable.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document applies.

BS EN ISO 9001:2000, *Quality management systems — Requirements*.

BS ISO/IEC 17799:2000, *Information technology — Code of practice for information security management*.

ISO Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*.

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1

availability

ensuring that authorized users have access to information and associated assets when required
[BS ISO/IEC 17799:2000]

3.2

confidentiality

ensuring that information is accessible only to those authorized to have access
[BS ISO/IEC 17799:2000]

3.3

information security

security preservation of confidentiality, integrity and availability of information

3.4
information security management system
ISMS

that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.5
integrity

safeguarding the accuracy and completeness of information and processing methods
[BS ISO/IEC 17799:2000]

3.6
risk acceptance

decision to accept a risk
[ISO Guide 73]

3.7
risk analysis

systematic use of information to identify sources and to estimate the risk
[ISO Guide 73]

3.8
risk assessment

overall process of risk analysis and risk evaluation
[ISO Guide 73]

3.9
risk evaluation

process of comparing the estimated risk against given risk criteria to determine the significance of risk
[ISO Guide 73]

3.10
risk management

coordinated activities to direct and control an organization with regard to risk
[ISO Guide 73]

3.11
risk treatment

treatment process of selection and implementation of measures to modify risk
[ISO Guide 73]

3.12
statement of applicability

document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes

4 Information security management system

4.1 General requirements

The organization shall develop, implement, maintain and continually improve a documented ISMS within the context of the organization's overall business activities and risk. For the purposes of this standard the process used is based on the PDCA model shown in Figure 1.

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS

The organization shall do the following.

- a) *Define the scope of the ISMS* in terms of the characteristics of the business, the organization, its location, assets and technology.
- b) *Define an ISMS policy* in terms of the characteristics of the business, the organization, its location, assets and technology that:
 - 1) includes a framework for setting its objectives and establishes an overall sense of direction and principles for action with regard to information security;
 - 2) takes into account business and legal or regulatory requirements, and contractual security obligations;
 - 3) establishes the strategic organizational and risk management context in which the establishment and maintenance of the ISMS will take place;
 - 4) establishes criteria against which risk will be evaluated and the structure of the risk assessment will be defined [see 4.2.1c)];
 - 5) has been approved by management.
- c) *Define a systematic approach to risk assessment*

Identify a method of risk assessment that is suited to the ISMS, and the identified business information security, legal and regulatory requirements. Set policy and objectives for the ISMS to reduce risks to acceptable levels. Determine criteria for accepting the risks and identify the acceptable levels of risk [see 5.1f)].

- d) *Identify the risks*
 - 1) Identify the assets within the scope of the ISMS and the owners of these assets.
 - 2) Identify the threats to those assets.
 - 3) Identify the vulnerabilities that might be exploited by the threats.
 - 4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.
- e) *Assess the risks*
 - 1) Assess the business harm that might result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the assets.
 - 2) Assess the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented.
 - 3) Estimate the levels of risks.
 - 4) Determine whether the risk is acceptable or requires treatment using the criteria established in 4.2.1c).
- f) *Identify and evaluate options for the treatment of risks*

Possible actions include:

- 1) applying appropriate controls;
- 2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and the criteria for risk acceptance [see 4.2.1c)];
- 3) avoiding risks;
- 4) transferring the associated business risks to other parties, e.g. insurers, suppliers.

g) *Select control objectives and controls for the treatment of risks*

Appropriate control objectives and controls shall be selected from Annex A of this standard and the selection shall be justified on the basis of the conclusions of the risk assessment and risk treatment process.

NOTE The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

h) *Prepare a Statement of Applicability*

The control objectives and controls selected in 4.2.1g) and the reasons for their selection shall be documented in the Statement of Applicability. The exclusion of any control objectives and controls listed in Annex A shall also be recorded.

i) Obtain management approval of the proposed residual risks and authorization to implement and operate the ISMS.

4.2.2 Implement and operate the ISMS

The organization shall do the following.

- a) Formulate a risk treatment plan that identifies the appropriate management action, responsibilities and priorities for managing information security risks (see Clause 5).
- b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.
- c) Implement controls selected in 4.2.1g) to meet the control objectives.
- d) Implement training and awareness programmes (see 5.2.2).
- e) Manage operations.
- f) Manage resources (see 5.2).
- g) Implement procedures and other controls capable of enabling prompt detection of and response to security incidents.

4.2.3 Monitor and review the ISMS

The organization shall do the following.

- a) Execute monitoring procedures and other controls to:
 - 1) detect errors in the results of processing promptly;
 - 2) identify failed and successful security breaches and incidents promptly;
 - 3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;
 - 4) determine the actions taken to resolve a breach of security reflecting business priorities.
- b) Undertake regular reviews of the effectiveness of the ISMS (including meeting security policy and objectives, and review of security controls) taking into account results of security audits, incidents, suggestions and feedback from all interested parties.
- c) Review the level of residual risk and acceptable risk, taking into account changes to:
 - 1) the organization;
 - 2) technology;
 - 3) business objectives and processes;
 - 4) identified threats;
 - 5) external events, such as changes to the legal or regulatory environment and changes in social climate.

- d) Conduct internal ISMS audits at planned intervals.
- e) Undertake a management review of the ISMS on a regular basis (at least once a year) to ensure that the scope remains adequate and improvements in the ISMS process are identified (see Clause 6).
- f) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).

4.2.4 *Maintain and improve the ISMS*

The organization shall regularly do the following.

- a) Implement the identified improvements in the ISMS.
- b) Take appropriate corrective and preventive actions in accordance with 7.2 and 7.3. Apply the lessons learnt from the security experiences of other organizations and those of the organization itself.
- c) Communicate the results and actions and agree with all interested parties.
- d) Ensure that the improvements achieve their intended objectives.

4.3 Documentation requirements

4.3.1 *General*

The ISMS documentation shall include the following.

- a) Documented statements of the security policy [see 4.2.1b)] and control objectives.
- b) The scope of the ISMS [see 4.2.1c)] and procedures and controls in support of the ISMS.
- c) Risk assessment report [see 4.2.1c) to 4.2.1g)].
- d) Risk treatment plan [see 4.2.2b)].
- e) Documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes (see 6.1).
- f) Records required by this British Standard (see 4.3.3).
- g) Statement of Applicability.

All documentation shall be made available as required by the ISMS policy.

NOTE 1 Where the term “documented procedure” appears within this standard, this means that the procedure is established, documented, implemented and maintained.

NOTE 2 The extent of the ISMS documentation can differ from one organization to another owing to:

- the size of the organization and the type of its activities;
- the scope and complexity of the security requirements and the system being managed.

NOTE 3 Documents and records may be in any form or type of medium.

4.3.2 *Control of documents*

Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:

- a) approve documents for adequacy prior to issue;
- b) review and update documents as necessary and re-approve documents;
- c) ensure that changes and the current revision status of documents are identified;
- d) ensure that the most recent versions of relevant documents are available at points of use;
- e) ensure that documents remain legible and readily identifiable;
- f) ensure that documents of external origin are identified;
- g) ensure that the distribution of documents is controlled;
- h) prevent the unintended use of obsolete documents;
- i) apply suitable identification to them if they are retained for any purpose.

4.3.3 Control of records

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be controlled. The ISMS shall take account of any relevant legal requirements. Records shall remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented. A management process shall determine the need for and extent of records.

Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of security incidents related to the ISMS.

EXAMPLE

Examples of records are a visitors' book, audit records and authorization of access.

5 Management responsibility

5.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

- a) establishing an information security policy;
- b) ensuring that information security objectives and plans are established;
- c) establishing roles and responsibilities for information security;
- d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
- e) providing sufficient resources to develop, implement, operate and maintain the ISMS (see 5.2.1);
- f) deciding the acceptable level of risk;
- g) conducting management reviews of the ISMS (see Clause 6).

5.2 Resource management

5.2.1 Provision of resources

The organization shall determine and provide the resources needed to:

- a) establish, implement, operate and maintain an ISMS;
- b) ensure that information security procedures support the business requirements;
- c) identify and address legal and regulatory requirements and contractual security obligations;
- d) maintain adequate security by correct application of all implemented controls;
- e) carry out reviews when necessary, and to react appropriately to the results of these reviews;
- f) where required, improve the effectiveness of the ISMS.

5.2.2 Training, awareness and competency

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

- a) determining the necessary competencies for personnel performing work effecting the ISMS;
- b) providing competent training and, if necessary, employing competent personnel to satisfy these needs;
- c) evaluating the effectiveness of the training provided and actions taken;
- d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

6 Management review of the ISMS

6.1 General

Management shall review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the security policy and security objectives. The results of the reviews shall be clearly documented and records shall be maintained (see 4.3.3).

6.2 Review input

The input to a management review shall include information on:

- a) results of ISMS audits and reviews;
- b) feedback from interested parties;
- c) techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;
- d) status of preventive and corrective actions;
- e) vulnerabilities or threats not adequately addressed in the previous risk assessment;
- f) follow-up actions from previous management reviews;
- g) any changes that could affect the ISMS;
- h) recommendations for improvement.

6.3 Review output

The output from the management review shall include any decisions and actions related to the following.

- a) Improvement of the effectiveness of the ISMS.
- b) Modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
 - 1) business requirements;
 - 2) security requirements;
 - 3) business processes effecting the existing business requirements;
 - 4) regulatory or legal environment;
 - 5) levels of risk and/or levels of risk acceptance.
- c) Resource needs.

6.4 Internal ISMS audits

The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:

- a) conform to the requirements of this standard and relevant legislation or regulations;
- b) conform to the identified information security requirements;
- c) are effectively implemented and maintained;
- d) perform as expected.

An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audits criteria, scope, frequency and methods shall be defined. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Improvement activities shall include the verification of the actions taken and the reporting of verification results (see Clause 7).

7 ISMS improvement

7.1 Continual improvement

The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

7.2 Corrective action

The organization shall take action to eliminate the cause of nonconformities associated with the implementation and operation of the ISMS in order to prevent recurrence. The documented procedures for corrective action shall define requirements for:

- a) identifying nonconformities of the implementation and/or operation of the ISMS;
- b) determining the causes of nonconformities;
- c) evaluating the need for actions to ensure that nonconformities do not recur;
- d) determining and implementing the corrective action needed;
- e) recording results of action taken (see 4.3.3);
- f) reviewing of corrective action taken.

7.3 Preventive action

The organization shall determine action to guard against future nonconformities in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:

- a) identifying potential nonconformities and their causes;
- b) determining and implementing preventive action needed;
- c) recording results of action taken (see 4.3.3);
- d) reviewing of preventive action taken;
- e) identifying changed risks and ensuring that attention is focused on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment.

NOTE Action to prevent nonconformities is often more cost-effective than corrective action.

Annex A (normative)

Control objectives and controls

A.1 Introduction

The control objectives and controls listed in **A.3** to **A.12** are directly derived from and aligned with those listed in BS ISO/IEC 17799:2000 Clauses **3** to **12**. The lists in these tables are not exhaustive and an organization may consider that additional control objectives and controls are necessary. Control objectives and controls from these tables shall be selected as part of the ISMS process specified in **4.2.1**.

A.2 Code of practice guidance

BS ISO/IEC 17799:2000 Clauses **3** to **12** provide implementation advice and guidance on best practice in support of the controls specified in **A.3** to **A.12**.

A.3 Security policy

			BS ISO/IEC 17799:2000 numbering
A.3.1 Information security policy			3.1
<i>Control objective:</i> To provide management direction and support for information security.			
<i>Controls</i>			
A.3.1.1	<i>Information security policy document</i>	A policy document shall be approved by management, published and communicated, as appropriate, to all employees.	3.1.1
A.3.1.2	<i>Review and evaluation</i>	The policy shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate	3.1.2

A.4 Organizational security

			BS ISO/IEC 17799:2000 numbering
A.4.1 Information security infrastructure			4.1
<i>Control objective:</i> To manage information security within the organization.			
<i>Controls</i>			
A.4.1.1	<i>Management information security forum</i>	A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place. The management forum shall promote security through appropriate commitment and adequate resourcing.	4.1.1
A.4.1.2	<i>Information security coordination</i>	In large organizations, a cross-functional forum of management representatives from relevant parts of the organization shall be used to coordinate the implementation of information security controls.	4.1.2
A.4.1.3	<i>Allocation of information security responsibilities</i>	Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.	4.1.3
A.4.1.4	<i>Authorization process for information processing facilities</i>	A management authorization process for new information processing facilities shall be established.	4.1.4
A.4.1.5	<i>Specialist information security advice</i>	Specialist advice on information security shall be sought from either internal or external advisors and coordinated throughout the organization.	4.1.5
A.4.1.6	<i>Cooperation between organizations</i>	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.	4.1.6
A.4.1.7	<i>Independent review of information security</i>	The implementation of the information security policy shall be reviewed independently.	4.1.7

A.4 (continued)

			BS ISO/IEC 17799:2000 numbering
A.4.2 Security of third-party access			4.2
<i>Control objective:</i> To maintain the security of organizational information processing facilities and information assets accessed by third parties.			
<i>Controls</i>			
A.4.2.1	<i>Identification of risks from third-party access</i>	The risks associated with access to organizational information processing facilities by third parties shall be assessed and appropriate security controls implemented.	4.2.1
A.4.2.2	<i>Security requirements in third-party contracts</i>	Arrangements involving third-party access to organizational information processing facilities shall be based on a formal contract containing all necessary security requirements.	4.2.2
A.4.3 Outsourcing			4.3
<i>Control objective:</i> To maintain the security of information when the responsibility for information processing has been outsourced to another organization.			
<i>Controls</i>			
A.4.3.1	<i>Security requirements in outsourcing contracts</i>	The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks and/or desktop environments shall be addressed in a contract agreed between the parties.	4.3.1

A.5 Asset classification and control

			BS ISO/IEC 17799:2000 numbering
A.5.1 Accountability for assets			5.1
<i>Control objective:</i> To maintain appropriate protection of organizational assets.			
<i>Controls</i>			
A.5.1.1	<i>Inventory of assets</i>	An inventory of all important assets associated with each information system shall be drawn up and maintained.	5.1.1
A.5.2 Information classification			5.2
<i>Control objective:</i> To ensure that information assets receive an appropriate level of protection.			
<i>Controls</i>			
A.5.2.1	<i>Classification guidelines</i>	Classifications and associated protective controls for information shall take account of business needs for sharing or restricting information, and the business impacts associated with such needs.	5.2.1
A.5.2.2	<i>Information labelling and handling</i>	A set of procedures shall be defined for information labelling and handling in accordance with the classification scheme adopted by the organization.	5.2.2

A.6 Personnel security

			BS ISO/IEC 17799:2000 numbering
A.6.1 Security in job definition and resourcing			6.1
<i>Control objective:</i> To reduce the risks of human error, theft, fraud or misuse of facilities.			
<i>Controls</i>			
A.6.1.1	<i>Including security in job responsibilities</i>	Security roles and responsibilities, as laid down in the organization's information security policy shall be documented in job definitions.	6.1.1
A.6.1.2	<i>Personnel screening and policy</i>	Verification checks on permanent staff, contractors, and temporary staff shall be carried out at the time of job applications.	6.1.2
A.6.1.3	<i>Confidentiality agreements</i>	Employees shall sign a confidentiality agreement as part of their initial terms and conditions of employment.	6.1.3
A.6.1.4	<i>Terms and conditions of employment</i>	The terms and conditions of employment shall state the employee's responsibility for information security.	6.1.4
A.6.2 User training			6.2
<i>Control objective:</i> To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.			
<i>Controls</i>			
A.6.2.1	<i>Information security education and training</i>	All employees of the organization and, where relevant, third-party users, shall receive appropriate training and regular updates in organizational policies and procedures.	6.2.1
A.6.3 Responding to security incidents and malfunctions			6.3
<i>Control objective:</i> To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.			
<i>Controls</i>			
A.6.3.1	<i>Reporting security incidents</i>	Security incidents shall be reported through appropriate management channels as quickly as possible.	6.3.1
A.6.3.2	<i>Reporting security weaknesses</i>	Users of information services shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services.	6.3.2
A.6.3.3	<i>Reporting software malfunctions</i>	Procedures shall be established for reporting software malfunctions.	6.3.3
A.6.3.4	<i>Learning from incidents</i>	Mechanisms shall be put in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.	6.3.4
A.6.3.5	<i>Disciplinary process</i>	The violation of organizational security policies and procedures by employees shall be dealt with through a formal disciplinary process.	6.3.5

A.7 Physical and environmental security

			BS ISO/IEC 17799:2000 numbering
A.7.1 Secure areas			7.1
<i>Control objective:</i> To prevent unauthorized physical access, damage and interference to business premises and information.			
<i>Controls</i>			
A.7.1.1	<i>Physical security perimeter</i>	Organizations shall use security perimeters to protect areas that contain information processing facilities.	7.1.1
A.7.1.2	<i>Physical entry controls</i>	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	7.1.2
A.7.1.3	<i>Securing offices, rooms and facilities</i>	Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.	7.1.3
A.7.1.4	<i>Working in secure areas</i>	Additional controls and guidelines for working in secure areas shall be used to enhance the security of secure areas.	7.1.4
A.7.1.5	<i>Isolated delivery and loading areas</i>	Delivery and loading areas shall be controlled, and where possible, isolated from information processing facilities to avoid unauthorized access.	7.1.5
A.7.2 Equipment security			7.2
<i>Control objective:</i> To prevent loss, damage or compromise of assets and interruption to business activities.			
<i>Controls</i>			
A.7.2.1	<i>Equipment siting and protection</i>	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	7.2.1
A.7.2.2	<i>Power supplies</i>	Equipment shall be protected from power failures and other electrical anomalies.	7.2.2
A.7.2.3	<i>Cabling security</i>	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	7.2.3
A.7.2.4	<i>Equipment maintenance</i>	Equipment shall be correctly maintained to enable its continued availability and integrity.	7.2.4
A.7.2.5	<i>Security of equipment off-premises</i>	Any use of equipment for information processing outside an organization's premises shall require authorization by management.	7.2.5
A.7.2.6	<i>Secure disposal or re-use of equipment</i>	Information shall be erased from equipment prior to disposal or re-use.	7.2.6
A.7.3 General controls			7.3
<i>Control objective:</i> To prevent compromise or theft of information and information processing facilities.			
<i>Controls</i>			
A.7.3.1	<i>Clear desk and clear screen policy</i>	Organizations shall have a clear desk and a clear screen policy aimed at reducing the risks of unauthorized access, loss of, and damage to information.	7.3.1
A.7.3.2	<i>Removal of property</i>	Equipment, information or software belonging to the organization shall not be removed without authorization of the management.	7.3.2

A.8 Communications and operations management

				BS ISO/IEC 17799:2000 numbering
A.8.1 Operational procedures and responsibilities				8.1
<i>Control objective:</i> To ensure the correct and secure operation of information processing facilities.				
<i>Controls</i>				
A.8.1.1	<i>Documented operating procedures</i>	The operating procedures identified in the security policy shall be documented and maintained.	8.1.1	
A.8.1.2	<i>Operational change controls</i>	Changes to information processing facilities and systems shall be controlled.	8.1.2	
A.8.1.3	<i>Incident management procedures</i>	Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents and to collect incident related data such as audit trails and logs.	8.1.3	
A.8.1.4	<i>Segregation of duties</i>	Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.	8.1.4	
A.8.1.5	<i>Separation of development and operational facilities</i>	Development and testing facilities shall be separated from operational facilities. Rules for the migration of software from development to operational status shall be defined and documented.	8.1.5	
A.8.1.6	<i>External facilities management</i>	Prior to using external facilities management services, the risks shall be identified and appropriate controls agreed with the contractor, and incorporated into a contract.	8.1.6	
A.8.2 System planning and acceptance				8.2
<i>Control objective:</i> To minimize the risk of systems failure.				
<i>Controls</i>				
A.8.2.1	<i>Capacity planning</i>	Capacity demands shall be monitored and projections of future capacity requirements made to enable adequate processing power and storage to be made available.	8.2.1	
A.8.2.2	<i>System acceptance</i>	Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance.	8.2.2	
A.8.3 Protection against malicious software				8.3
<i>Control objective:</i> To protect the integrity of software and information from damage by malicious software.				
<i>Controls</i>				
A.8.3.1	<i>Controls against malicious software</i>	Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.	8.3.1	
A.8.4 Housekeeping				8.4
<i>Control objective:</i> To maintain the integrity and availability of information processing and communication services.				
<i>Controls</i>				
A.8.4.1	<i>Information back-up</i>	Back-up copies of essential business information and software shall be taken and tested regularly.	8.4.1	

A.8 (continued)

			BS ISO/IEC 17799:2000 numbering
A.8.4.2	<i>Operator logs</i>	Operational staff shall maintain a log of their activities. Operator logs shall be subject to regular, independent checks.	8.4.2
A.8.4.3	<i>Fault logging</i>	Faults shall be reported and corrective action taken.	8.4.3
A.8.5 Network management			8.5
<i>Control objective:</i> To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.			
<i>Controls</i>			
A.8.5.1	<i>Network controls</i>	A range of controls shall be implemented to achieve and maintain security in networks.	8.5.1
A.8.6 Media handling and security			8.6
<i>Control objective:</i> To prevent damage to assets and interruptions to business activities.			
<i>Controls</i>			
A.8.6.1	<i>Management of removable computer media</i>	The management of removable computer media, such as tapes, disks, cassettes and printed reports shall be controlled.	8.6.1
A.8.6.2	<i>Disposal of media</i>	Media shall be disposed of securely and safely when no longer required.	8.6.2
A.8.6.3	<i>Information handling procedures</i>	Procedures for the handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse.	8.6.3
A.8.6.4	<i>Security of system documentation</i>	System documentation shall be protected from unauthorized access.	8.6.4
A.8.7 Exchanges of information and software			8.7
<i>Control objective:</i> To prevent loss, modification or misuse of information exchanged between organizations.			
<i>Controls</i>			
A.8.7.1	<i>Information and software exchange agreements</i>	Agreements, some of which may be formal, shall be established for the exchange of information and software (whether electronic or manual) between organizations.	8.7.1
A.8.7.2	<i>Security of media in transit</i>	Media being transported shall be protected from unauthorized access, misuse or corruption.	8.7.2
A.8.7.3	<i>Electronic commerce security</i>	Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.	8.7.3
A.8.7.4	<i>Security of electronic mail</i>	A policy for the use of electronic mail shall be developed and controls put in place to reduce security risks created by electronic mail.	8.7.4
A.8.7.5	<i>Security of electronic office systems</i>	Policies and guidelines shall be prepared and implemented to control the business and security risks associated with electronic office systems.	8.7.5
A.8.7.6	<i>Publicly available systems</i>	There shall be a formal authorization process before information is made publicly available and the integrity of such information shall be protected to prevent unauthorized modification.	8.7.6
A.8.7.7	<i>Other forms of information exchange</i>	Policies, procedures and controls shall be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.	8.7.7

A.9 Access control

			BS ISO/IEC 17799:2000 numbering
A.9.1 Business requirement for access control			9.1
<i>Control objective:</i> To control access to information.			
<i>Controls</i>			
A.9.1.1	<i>Access control policy</i>	Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.	9.1.1
A.9.2 User access management			9.2
<i>Control objective:</i> To ensure that access rights to information systems are appropriately authorized, allocated and maintained.			
<i>Controls</i>			
A.9.2.1	<i>User registration</i>	There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.	9.2.1
A.9.2.2	<i>Privilege management</i>	The allocation and use of privileges shall be restricted and controlled.	9.2.2
A.9.2.3	<i>User password management</i>	The allocation of passwords shall be controlled through a formal management process.	9.2.3
A.9.2.4	<i>Review of user access rights</i>	Management shall conduct a formal process at regular intervals to review users' access rights.	9.2.4
A.9.3 User responsibilities			9.3
<i>Control objective:</i> To prevent unauthorized user access.			
<i>Controls</i>			
A.9.3.1	<i>Password use</i>	Users shall be required to follow good security practices in the selection and use of passwords.	9.3.1
A.9.3.2	<i>Unattended user equipment</i>	Users shall be required to ensure that unattended equipment is given appropriate protection.	9.3.2
A.9.4 Network access control			9.4
<i>Control objective:</i> Protection of networked services.			
<i>Controls</i>			
A.9.4.1	<i>Policy on use of network services</i>	Users shall only have direct access to the services that they have been specifically authorized to use.	9.4.1
A.9.4.2	<i>Enforced path</i>	The path from the user terminal to the computer service shall be controlled.	9.4.2
A.9.4.3	<i>User authentication for external connections</i>	Access by remote users shall be subject to authentication.	9.4.3
A.9.4.4	<i>Node authentication</i>	Connections to remote computer systems shall be authenticated.	9.4.4
A.9.4.5	<i>Remote diagnostic port protection</i>	Access to diagnostic ports shall be securely controlled.	9.4.5
A.9.4.6	<i>Segregation in networks</i>	Controls shall be introduced in networks to segregate groups of information services, users and information systems.	9.4.6
A.9.4.7	<i>Network connection control</i>	The connection capability of users shall be restricted in shared networks, in accordance with the access control policy.	9.4.7
A.9.4.8	<i>Network routing control</i>	Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.	9.4.8

A.9 (continued)

			BS ISO/IEC 17799:2000 numbering
A.9.4.9	<i>Security of network services</i>	A clear description of the security attributes of all network services used by the organization shall be provided.	9.4.9
A.9.5 Operating system access control			9.5
<i>Control objective:</i> To prevent unauthorized computer access.			
<i>Controls</i>			
A.9.5.1	<i>Automatic terminal identification</i>	Automatic terminal identification shall be considered to authenticate connections to specific locations and to portable equipment.	9.5.1
A.9.5.2	<i>Terminal log-on procedures</i>	Access to information services shall use a secure log-on process.	9.5.2
A.9.5.3	<i>User identification and authentication</i>	All users shall have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual. A suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	9.5.3
A.9.5.4	<i>Password management system</i>	Password management systems shall provide an effective, interactive facility which aims to ensure quality passwords.	9.5.4
A.9.5.5	<i>Use of system utilities</i>	Use of system utility programs shall be restricted and tightly controlled.	9.5.5
A.9.5.6	<i>Duress alarm to safeguard users</i>	Duress alarms shall be provided for users who might be the target of coercion.	9.5.6
A.9.5.7	<i>Terminal time-out</i>	Inactive terminals in high risk locations or serving high risk systems shall shut down after a defined period of inactivity to prevent access by unauthorized persons.	9.5.7
A.9.5.8	<i>Limitation of connection time</i>	Restrictions on connection times shall be used to provide additional security for high risk applications.	9.5.8
A.9.6 Application access control			9.6
<i>Control objective:</i> To prevent unauthorized access to information held in information systems.			
<i>Controls</i>			
A.9.6.1	<i>Information access restriction</i>	Access to information and application system functions shall be restricted in accordance with the access control policy.	9.6.1
A.9.6.2	<i>Sensitive system isolation</i>	Sensitive systems shall have a dedicated (isolated) computing environment.	9.6.2
A.9.7 Monitoring system access and use			9.7
<i>Control objective:</i> To detect unauthorized activities.			
<i>Controls</i>			
A.9.7.1	<i>Event logging</i>	Audit logs recording exceptions and other security-relevant events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	9.7.1
A.9.7.2	<i>Monitoring system use</i>	Procedures for monitoring the use of information processing facilities shall be established and the result of the monitoring activities reviewed regularly.	9.7.2
A.9.7.3	<i>Clock synchronization</i>	Computer clocks shall be synchronized for accurate recording	9.7.3

A.9 (continued)

			BS ISO/IEC 17799:2000 numbering
A.9.8 Mobile computing and teleworking			9.8
<i>Control objective:</i> To ensure information security when using mobile computing and teleworking facilities.			
<i>Controls</i>			
A.9.8.1	<i>Mobile computing</i>	A formal policy shall be in place and appropriate controls shall be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.	9.8.1
A.9.8.2	<i>Teleworking</i>	Policies, procedures and standards shall be developed to authorize and control teleworking activities.	9.8.2

A.10 System development and maintenance

			BS ISO/IEC 17799:2000 numbering
A.10.1 Security requirements of systems			10.1
<i>Control objective:</i> To ensure that security is built into information systems.			
<i>Controls</i>			
A.10.1.1	<i>Security requirements analysis and specification</i>	Business requirements for new systems, or enhancements to existing systems shall specify the requirements for controls.	10.1.1
A.10.2 Security in application systems			10.2
<i>Control objective:</i> To prevent loss, modification or misuse of user data in application systems.			
<i>Controls</i>			
A.10.2.1	<i>Input data validation</i>	Data input to application systems shall be validated to ensure that it is correct and appropriate.	10.2.1
A.10.2.2	<i>Control of internal processing</i>	Validation checks shall be incorporated into systems to detect any corruption of the data processed.	10.2.2
A.10.2.3	<i>Message authentication</i>	Message authentication shall be used for applications where there is a security requirement to protect the integrity of the message content.	10.2.3
A.10.2.4	<i>Output data validation</i>	Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	10.2.4
A.10.3 Cryptographic controls			10.3
<i>Control objective:</i> To protect the confidentiality, authenticity or integrity of information.			
<i>Controls</i>			
A.10.3.1	<i>Policy on the use of cryptographic controls</i>	A policy on the use of cryptographic controls for the protection of information shall be developed.	10.3.1
A.10.3.2	<i>Encryption</i>	Encryption shall be applied to protect the confidentiality of sensitive or critical information.	10.3.2
A.10.3.3	<i>Digital signatures</i>	Digital signatures shall be applied to protect the authenticity and integrity of electronic information.	10.3.3
A.10.3.4	<i>Non-repudiation services</i>	Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event or action.	10.3.4
A.10.3.5	<i>Key management</i>	A key management system based on an agreed set of standards, procedures and methods shall be used to support the use of cryptographic techniques.	10.3.5

A.10 (continued)

			BS ISO/IEC 17799:2000 numbering
A.10.4 Security of system files			10.4
<i>Control objective:</i> To ensure that IT projects and support activities are conducted in a secure manner.			
<i>Controls</i>			
A.10.4.1	<i>Control of operational software</i>	Procedures shall be in place to control the implementation of software on operational systems.	10.4.1
A.10.4.2	<i>Protection of system test data</i>	Test data shall be protected and controlled.	10.4.2
A.10.4.3	<i>Access control to program source library</i>	Strict control shall be maintained over access to program source libraries.	10.4.3
A.10.5 Security in development and support processes			10.5
<i>Control objective:</i> To maintain the security of application system software and information.			
<i>Controls</i>			
A.10.5.1	<i>Change control procedures</i>	The implementation of changes shall be strictly controlled by the use of formal change control procedures.	10.5.1
A.10.5.2	<i>Technical review of operating system changes</i>	Application systems shall be reviewed and tested when changes occur.	10.5.2
A.10.5.3	<i>Restrictions on changes to software packages</i>	Modifications to software packages shall be discouraged and essential changes strictly controlled.	10.5.3
A.10.5.4	<i>Covert channels and Trojan code</i>	The purchase, use and modification of software shall be controlled and checked to protect against possible covert channels and Trojan code.	10.5.4
A.10.5.5	<i>Outsourced software development</i>	Controls shall be applied to secure outsourced software development.	10.5.5

A.11 Business continuity management

			BS ISO/IEC 17799:2000 numbering
A.11.1 Aspects of business continuity management			11.1
<i>Control objective:</i> To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.			
<i>Controls</i>			
A.11.1.1	<i>Business continuity management process</i>	There shall be a managed process in place for developing and maintaining business continuity throughout the organization.	11.1.1
A.11.1.2	<i>Business continuity and impact analysis</i>	A strategy plan, based on appropriate risk assessment, shall be developed for the overall approach to business continuity.	11.1.2
A.11.1.3	<i>Writing and implementing continuity plans</i>	Plans shall be developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes.	11.1.3
A.11.1.4	<i>Business continuity planning framework</i>	A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.	11.1.4
A.11.1.5	<i>Testing, maintaining and re-assessing business continuity plans</i>	Business continuity plans shall be tested regularly and maintained by regular reviews to ensure that they are up to date and effective.	11.1.5

A.12 Compliance

			BS ISO/IEC 17799:2000 numbering
A.12.1 Compliance with legal requirements			12.1
<i>Control objective:</i> To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.			
<i>Controls</i>			
A.12.1.1	<i>Identification of applicable legislation</i>	All relevant statutory, regulatory and contractual requirements shall be defined explicitly and documented for each information system.	12.1.1
A.12.1.2	<i>Intellectual property rights (IPR)</i>	Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.	12.1.2
A.12.1.3	<i>Safeguarding of organizational records</i>	Important records of an organization shall be protected from loss, destruction and falsification.	12.1.3
A.12.1.4	<i>Data protection and privacy of personal information</i>	Controls shall be applied to protect personal information in accordance with relevant legislation.	12.1.4
A.12.1.5	<i>Prevention of misuse of information processing facilities</i>	Management shall authorize the use of information processing facilities and controls shall be applied to prevent the misuse of such facilities.	12.1.5
A.12.1.6	<i>Regulation of cryptographic controls</i>	Controls shall be in place to enable compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls.	12.1.6
A.12.1.7	<i>Collection of evidence</i>	Where action against a person or organization involves the law, either civil or criminal, the evidence presented shall conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard. This shall include compliance with any published standard or code of practice for the production of admissible evidence.	12.1.7
A.12.2 Reviews of security policy and technical compliance			12.2
<i>Control objective:</i> To ensure compliance of systems with organizational security policies and standards.			
<i>Controls</i>			
A.12.2.1	<i>Compliance with security policy</i>	Managers shall take action to ensure that all security procedures within their area of responsibility are carried out correctly and all areas within the organization shall be subject to regular review to ensure compliance with security policies and standards.	12.2.1
A.12.2.2	<i>Technical compliance checking</i>	Information systems shall be regularly checked for compliance with security implementation standards.	12.2.2
A.12.3 System audit considerations			12.3
<i>Control objective:</i> To maximize the effectiveness of and to minimize interference to/from the system audit process.			
<i>Controls</i>			
A.12.3.1	<i>System audit controls</i>	Audits of operational systems shall be planned carefully and agreed to minimize the risk of disruptions to business processes.	12.3.1
A.12.3.2	<i>Protection of system audit tools</i>	Access to system audit tools shall be protected to prevent any possible misuse or compromise.	12.3.2

Annex B (informative)

Guidance on use of the standard

B.1 Overview

B.1.1 PDCA model

Setting up and managing an ISMS requires the same approach(es) as for any other management system. The process model described here follows a continuous cycle of activities: Plan, Do, Check, and Act. This can be described as a virtuous cycle because its purpose is to ensure that the best practices of your organization are documented, reinforced and improved with time.

B.1.2 Plan and Do

A process of continual improvement often requires an initial investment: documenting practices, formalizing the approach to risk management, determining methods of review and allocating resources. These activities are used to “kick start” the cycle. They do not need to be completed before the review phases can become active. The Plan phase is used to ensure that the context and scope for the ISMS have been correctly established, that the information security risks are assessed and that a plan for the appropriate treatment of these risks is developed. The Do phase is used to implement the decisions made and solutions identified in the Plan phase.

B.1.3 Check and Act

The Check and Act review phases are used to reinforce, amend and improve the security solutions identified and implemented already. The reviews can take place at any time and frequency, depending on what is most appropriate for the situation considered. In some systems they may have to be built into computerized processes to operate and respond immediately. Other processes will be needed to respond only when there is a security failure, where changes or additions are made to the information assets being protected, and when changes to threats and vulnerabilities occur. Finally, annual or other periodic reviews or audits are needed to ensure that the whole management system is achieving its objectives.

B.1.4 Summary of controls

The organization may find it beneficial to make available a Summary of Controls (SoC) that is relevant and applicable to the organization's ISMS. This can facilitate business relationships such as electronic outsourcing by providing a summary of the controls in place. The SoC may contain sensitive information. Therefore care that it is appropriate to the recipient should be taken when making the SoC available both internally and externally.

NOTE The SoC is not a substitute for the SoA [see 4.2.1h)]. The SoA is a mandatory requirement for certification.

B.2 Plan phase

B.2.1 Introduction

The Plan activity of the Plan, Do, Check and Act cycle is designed to ensure that the context and scope for the ISMS have been correctly established, that all information security risks are identified and assessed, and that a plan for the appropriate treatment of these risks is developed. It is important that all stages of the Plan activity are documented for traceability and for the management of change.

B.2.2 Information security policy

4.2.1b) requires the organization and its management to define the information security policy that includes a framework for setting its objectives and targets, and establishes an overall sense of direction and principles for action with regard to information security. Guidance on the content of such a policy is given in BS ISO/IEC 17799:2000.

B.2.3 Scope of the ISMS

The ISMS may cover all or part of an organization. Dependencies, interfaces and assumptions concerning the boundary with the environment need to be clearly identified. This is particularly relevant if only part of an organization is within the scope of the ISMS. The scope may be divided in some way, for example into domains to make subsequent risk management tasks simpler. The ISMS scope documentation should cover:

- a) the processes used to establish the scope and context of the ISMS;
- b) the strategic and organizational context(s);
- c) the organization's approach to information security risk management;
- d) criteria for information security risk evaluation and the degree of assurance required;
- e) identification of the information assets within the scope of the ISMS.

The ISMS may fall within the scope of control of a Quality Management System, another Management System or another ISMS (of the same or a third-party organization). In such cases, only those controls the ISMS has management control over can be considered as being within the scope of the ISMS.

B.2.4 Risk identification and assessment

The risk assessment documentation should explain which risk assessment approach has been chosen, and why this approach is appropriate to the security requirements, the business environment, the size of the business and the risks the organization faces. The approach adopted should aim to focus security effort and resources in a cost-effective and efficient way. The documentation should also cover the tools and techniques that have been chosen, explain why they are suitable for the ISMS scope and risks, and how they should be used correctly to produce valid results.

The following risk assessment details should be documented:

- a) the valuation of the assets within the ISMS, including information about the valuation scale used, when it is not monetary;
- b) identification of threats and vulnerabilities;
- c) assessment of threats exploiting vulnerabilities, and of the impacts caused by such incidents;
- d) calculation of the risks based on the results of the assessment, and identification of residual risks.

B.2.5 Risk treatment plan

Organizations should create a detailed schedule, or risk treatment plan, showing for each identified risk:

- a) the method selected for treating the risk;
- b) what controls are in place;
- c) what additional controls are proposed;
- d) the time frame over which the proposed controls are to be implemented.

An acceptable level of risk needs to be identified. For each of the risks at an unacceptable level, appropriate action should be chosen from the following:

- a) decide to accept the risk, e.g. because other actions are not possible or too expensive;
- b) transfer the risk; or
- c) reduce the risk to an acceptable level.

The risk treatment plan is a coordination document defining the actions to reduce unacceptable levels of risk and implement the controls required to protect information.

It might not always be possible to reduce risks to an acceptable level within an acceptable cost, and then a decision should be made whether to add more controls, or accept the higher risks. When setting an acceptable level of risk the strength and cost of control should be compared with the potential cost of an incident.

The Statement of Applicability [see 4.2.1h)] documents the control objectives and controls selected from Annex A. This document is one of the working documents required for ISMS certification. BS ISO/IEC 17799:2000 provides additional information relevant to implementing these controls.

Additional controls may need to be designed and implemented where the identified risks exceed the level that can be managed with those controls.

Controls designed to deter, detect, limit, prevent and recover from, security violations (in accordance with the ISMS) are very important in the implementation of the PDCA model and should be put in place early enough to be effective, along with those governing controls providing prevention, deterrence, limitation and recovery.

The plan should include a schedule and priorities, a detailed work plan and responsibilities for the implementation of controls.

B.3 Do phase

B.3.1 Introduction

The Do activity within the PDCA cycle is designed to implement selected controls and promote the action necessary to manage the information security risks in line with the decisions that have been taken in the Plan phase.

B.3.2 Resources, training and awareness

Adequate resources (people, time and money) should be allocated to the operation of the ISMS and all security controls. This includes the documentation of all controls that have been implemented, and active maintenance of the ISMS documentation. In addition, security awareness and training programmes should be put in place, in parallel with the implementation of the security controls.

The aim of the awareness programme is to generate a well-founded risk management and security culture. The success of the awareness programme should be monitored to ensure its continual effectiveness and topicality. Specific security training should be applied wherever necessary to support the awareness programme, and to enable all interested parties to fulfil their security tasks as required.

B.3.3 Risk treatment

For those risks that have been assessed as acceptable, no further action is needed.

If the decision has been made to transfer risks, the necessary actions should be taken, e.g. using contracts, insurance arrangements and organizational structures such as partnership and joint ventures. In such cases, it should be ensured that the organization(s) to which the risks are transferred understand the nature of those risks and are able to manage them effectively.

Wherever the decision has been made to reduce the risks, the controls that have been selected need to be implemented. This should take place in line with the risk treatment plan prepared in the Plan activity. The successful implementation of the plan requires an effective management system, which specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria. Where a business has decided to accept risks that are higher than the acceptance level, sign-off from management should be obtained.

After unacceptable risks have been reduced or transferred, there may be residual risks that are retained. Controls should ensure that undesirable impacts or breaches are promptly identified and appropriately managed.

B.4 Check phase

B.4.1 Introduction

The Check activity is designed to ensure that the controls are working effectively and as intended, and that the ISMS remains effective. In addition, any change to the assumptions or scope of the risk assessment should be considered. If the controls are found inadequate then the necessary corrective action needs to be determined. The execution of such actions is the subject of the Act phase of the PDCA cycle. It is important to realize that corrective action is only necessary:

- a) to maintain internal consistency of the ISMS documentation; and
- b) if the effect of not making the change would result in exposing the organization to an unacceptable risk.

The Check activity should also include a description of procedures for the management and operation of the controls in the ISMS and processes for ongoing review of risks and their treatment in the light of changing technology, threats, or functions.

Whilst it may be determined that the current state of security is satisfactory, attention should be paid to changing technology and business requirements and the onset of new threats and vulnerabilities, in order to anticipate future changes to the ISMS and ensure its continued effectiveness in the future.

The information collected during the Check phase provides a valuable source of data that can be used to determine and measure the effectiveness of the ISMS in meeting the documented security policy and objectives of the organization. It should also be used as a source to identify inefficient and ineffective processes and procedures.

The nature of the Check activity depends on the character of the PDCA cycle concerned, as in the following examples:

EXAMPLE 1

The automatic actions of intrusion detection technology. A network intrusion detector checks whether the security of other components has been penetrated.

EXAMPLE 2

The actions resulting from a security incident. Procedures for taking action in the event of a security incident may well disclose where controls have failed or where additional controls are required.

Other examples are given in **B.4.2** to **B.4.7**.

B.4.2 Routine checking

These procedures are performed on a regular basis as part of the normal business process and are designed to detect errors in the results of processing. They might include: reconciliation of bank accounts, inventory counts, and resolving customer complaints. Clearly checks of this type need to be designed into systems to be performed often enough to limit any damage (and consequent liability) from any errors that occur.

In today's systems this type of check might be extended to include:

- a) checks that there are no unintended and unauthorized changes to parameters governing the actions of software, that there are no unintended and unauthorized changes to data displayed on websites;
- b) confirmation of completeness and accuracy of transfers of data between parties in "virtual" companies in cyberspace.

B.4.3 Self-policing procedures

A self-policing procedure is a control that has been constructed so that any error, or failure perpetrated during execution is capable of prompt detection. An example would be a device that monitors a network (e.g. for equipment failures or errors) and raises an alarm. The alarm alerts the responsible people to the problem, and they then have the task of diagnosing the cause of the problem and fixing it. However if the problem is not corrected within a defined period of time additional alarms are raised to more senior management, thus escalating the problem automatically.

B.4.4 Learning from others

One way to identify where the organization's procedures are suboptimal is to identify where other organizations deal with problems more effectively. This learning applies both to the technical software and to the management activities. There are many sources that identify vulnerabilities in technology and software. Organizations should refer to these frequently and make the necessary updates to their software.

Information on management techniques is exchanged and discussed in many forums, including conferences, professional societies, and user groups and there are many articles in the technical and management press. Such exchanges enable organizations to learn how others tackle similar problems.

B.4.5 Internal ISMS audit

The overall objective is to check over a specified regular audit period (which should last no more than one year) that all aspects of the ISMS are functioning as intended. A sufficient number of audits should be planned so that the audit task is spread uniformly over the chosen period. Management should ensure that there is evidence that confirms that:

- a) the information security policy is still an accurate reflection of the business requirements;
- b) an appropriate risk assessment methodology is being used;
- c) the documented procedures are being followed (i.e. within the scope of the ISMS), and are meeting their desired objectives;
- d) technical controls (e.g. firewalls, physical access controls) are in place, are correctly configured and working as intended;
- e) the residual risks have been assessed correctly and are still acceptable to the management of the organization;
- f) the agreed actions from previous audits and reviews have been implemented;
- g) the ISMS is compliant with this standard.

The audits will need samples of current documents and records and involve interviews with management and staff.

B.4.6 Management review

The overall objective is to check, at least once per year, that the ISMS is effective, to identify where improvements can be made and to take action. Whilst it may be determined that the current state of security is satisfactory, attention should be paid to changing technology and business requirements and the onset of new threats and vulnerabilities in order to anticipate future changes to the ISMS and ensure its continued effectiveness.

B.4.7 Trend analysis

Trend analysis undertaken on a regular basis will help organizations identify those areas in which a need for improvement is indicated and should form an essential part of the continuous improvement cycle.

B.5 Act phase

B.5.1 Introduction

In order for the ISMS to remain effective it should be regularly improved on the basis of information collected during the Check phase.

The purpose of the Act activity is to take action as a result of the Check activity. The action will be to address a nonconformity or take other corrective action as explained in **B.5.2** and **B.5.3**. The action might also be to advance immediately to a Plan or Do activity. An example of the former would be when a new threat has been identified, the Plan activity being to update the risk assessment. An example of the latter would be to put an existing business continuity plan into action, the Check activity having identified the need to do that. Note that if changes are made to the ISMS as a result of the Act or subsequent Plan activities, then it is vital that all interested parties are advised promptly about the changes and that additional training should be given as required.

B.5.2 Nonconformity

A nonconformity (from the application guidance to the clauses of ISO/IEC Guide 62) is:

- a) the absence of, or the failure to implement and maintain one or more ISMS requirements; or
- b) a situation which would, on the basis of available objective evidence, raise significant doubt as to the capability of the ISMS to fulfil the information security policy and security objectives of the organization.

It is important that where reviews during the Check phase highlight areas of nonconformity, further investigations are conducted to identify the root cause of the event and actions are identified not only to resolve the issue but also to minimize and prevent recurrence. Corrective action should be consistent with the severity of the nonconformity and the risk to the ability of the ISMS to meet specified requirements.

B.5.3 Corrective and preventive actions

Corrective (or reactive) action should be taken to eliminate the cause of a nonconformity or other undesirable situation to prevent recurrence. Preventive (or proactive) action should be taken to eliminate the cause of a potential noncompliance or other undesirable potential situation.

It is never possible to entirely eliminate isolated nonconformities. On the other hand, what may appear to be an isolated event may in fact be symptomatic of a weakness that may have an impact across the entire organization if not addressed. Isolated events should be considered from this point of view when identifying and implementing any corrective actions. In addition to the immediate corrective actions identified, it is important to consider the medium- to long-term view, ensuring the remedial work not only addresses the issue under consideration but also prevents or reduces the likelihood of a similar event recurring.

B.5.4 OECD principles and BS 7799-2:2002

The principles given in the OECD Guidelines for the Security of Information Systems and Networks [1] apply to all policy and operational levels that govern the security of information systems and networks. This British Standard provides an information security management system framework for implementing some of the OECD principles using the PDCA model and the processes described in Clauses 4, 5, 6 and 7, as indicated in Table B.1.

Table B.1 — OECD principles and the PDCA model

OECD principle	Corresponding ISMS process and PDCA phase
Awareness Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.	This activity is part of the Do phase (see 4.2.2 and 5.2.2).
Responsibility All participants are responsible for the security of information systems and networks.	This activity is part of the Do phase (see 4.2.2 and 5.1).
Response Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.	This is in part a monitoring activity Check phase (see 4.2.3 and 6.1 to 6.4) and a responding activity Act phase (see 4.2.4 and 7.1 to 7.3). This can also be covered by some aspects of the Plan and Check phases.
Risk assessment Participants should conduct risk assessments.	This activity is part of the Plan phase (see 4.2.1) and risk reassessment is part of the Check phase (see 4.2.3 and 6.1 to 6.4).
Security design and implementation Participants should incorporate security as an essential element of information systems and networks.	Once a risk assessment has been completed, controls are selected for the treatment of risks as part of the Plan phase (see 4.2.1). The Do phase (see 4.2.2 and 5.2) then covers the implementation and operational use of these controls.
Security management Participants should adopt a comprehensive approach to security management.	The management of risk is a process which includes the prevention, detection and response to incidents, ongoing maintenance, review and audit. All of these aspects are encompassed in the Plan, Do, Check and Act phases.
Reassessment Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.	Reassessment of information security is a part of the Check phase (see 4.2.3 and 6.1 to 6.4) where regular reviews should be undertaken to check the effectiveness of the information security management system, and improving the security is part of the Act phase (see 4.2.4 and 7.1 to 7.3).

Annex C (informative)**Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002**

Table C.1 shows the correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002.

Table C.1 — Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002

BS 7799-2:2002	BS EN ISO 9001:2000	BS EN ISO 14001:1996
0 Introduction	0 Introduction	Introduction
0.1 General	0.1 General	
0.2 Process approach	0.2 Process approach	
	0.3 Relationship with ISO 9004	
0.3 Compatibility with other management systems	0.4 Compatibility with other management systems	
1 Scope	1 Scope	1 Scope
1.1 General	1.1 General	
1.2 Application	1.2 Application	
2 Normative references	2 Normative reference	2 Normative reference
3 Terms and definitions	3 Terms and definitions	3 Terms and definitions
4 ISMS requirements	4 QMS requirements	4 EMS requirements
4.1 General requirements	4.1 General requirements	4.1 General requirements
4.2 Establishing and managing the ISMS		
4.2.1 Establish the ISMS		
4.2.2 Implement and operate the ISMS		4.4 Implementation and operation
4.2.3 Monitor and review the ISMS		4.5.1 Monitoring and measurement
4.2.4 Maintain and improve the ISMS		4.5.2 Non-conformance and corrective and preventive action
4.3 Documentation requirements	4.2 Documentation requirements	
4.3.1 General	4.2.1 General	
	4.2.2 Quality manual	
4.3.2 Control of documents	4.2.3 Control of documents	4.4.5 Documentation control
4.3.3 Control of records	4.2.4 Control of records	4.5.3 Records
5 Management responsibility	5 Management responsibility	
5.1 Management commitment	5.1 Management commitment	
	5.2 Customer focus	
	5.3 Quality policy	4.2 Environmental policy
	5.4 Planning	4.3 Planning
	5.5 Responsibility, authority and communication	

Table C.1 — Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002 (concluded)

BS 7799-2:2002	BS EN ISO 9001:2000	BS EN ISO 14001:1996
5.2 Resource management 5.2.1 Provision of resources 5.2.2 Training, awareness and competency	6 Resource management 6.1 Provision of resources 6.2 Human resources 6.2.2 Competence, awareness and training 6.3 Infrastructure 6.4 Work environment	4.2.2 Training, awareness and competence
6 Management review of the ISMS 6.1 General 6.2 Review input 6.3 Review output 6.4 Internal ISMS audits	5.6 Management review 5.6.1 General 5.6.2 Review input 5.6.3 Review output 8.2.2 Internal audits	4.6 Management review 4.5.4 EMS audit
7 ISMS improvement 7.1 Continual improvement 7.2 Corrective action 7.3 Preventive action	8 Improvement 8.5.1 Continual improvement 8.5.2 Corrective actions 5.5.3 Preventive actions	4.5.2 Non-conformance and corrective and preventive action
Annex A Control objectives and controls Annex B Guidance on use of the standard Annex C Correspondence between different management system standards	Annex A Links between ISO 14001 and ISO 9001	Annex A Guidance on use of the specification Annex B Links between ISO 14001 and ISO 9001

Annex D (informative)

Changes to internal numbering

Table D.1 shows the relationship between the clause numbering in BS 7799-2:1999 and the clause numbering in this British Standard, BS 7799-2:2002.

Table D.1 — Relationship between internal numbering in different editions of BS 7799-2

Clause number in BS 7799-2:1999	Clause number in BS 7799-2:2002
—	0 Introduction
1 Scope	1 Scope
—	2 Normative references
2 Terms and definitions	3 Terms and definitions
—	3.1 Information security management system
2.1 Statement of applicability	3.12 Statement of applicability
3 Information security management system requirements	4 Information security management system
3.1 General	4.1 General requirements
3.2 Establishing a management framework	4.2 Establishing and managing the ISMS
—	4.2.1 Establish the ISMS
3.3 Implementation	4.2.2 Implement and operate the ISMS
—	4.2.3 Monitor and review the ISMS
—	4.2.4 Maintain and improve the ISMS
3.4 Documentation	4.3 Documentation requirements
—	4.3.1 General
3.5 Document control	4.3.2 Control of documents
3.6 Records	4.3.3 Control of records
—	5 Management responsibility
—	5.1 Management commitment
—	5.2 Resource management
—	6 Management review of the ISMS
—	6.1 General
—	6.2 Review input
—	6.3 Review output
—	6.4 Internal ISMS audits
—	7 ISMS improvement
—	7.1 Continual improvement
—	7.2 Corrective action
—	7.3 Preventive action
4 Detailed controls	Annex A Control objectives and controls
—	A.1 Introduction
—	A.2 Code of practice guidance
4.1 Security policy	A.3 Security policy
4.2 Organizational security	A.4 Organizational security
4.3 Asset classification and control	A.5 Asset classification and control
4.4 Personnel security	A.6 Personnel security
4.5 Physical and environmental security	A.7 Physical and environmental security

Table D.1 — Relationship between internal numbering in different editions of BS 7799-2 (concluded)

Clause number in BS 7799-2:1999	Clause number in BS 7799-2:2002
4.6 Communications and operations management	A.8 Communications and operations management
4.7 Access control	A.9 Access control
4.8 System development and maintenance	A.10 System development and maintenance
4.9 Business continuity management	A.11 Business continuity management
4.10 Compliance	A.12 Compliance
—	Annex B Guidance on the use of the standard
—	Annex C Correspondence between BS EN ISO 9001:2000, BS EN ISO 14001:1996 and BS 7799-2:2002

Bibliography

Standards publications

BS 7799-2:1999, *Information security management — Part 2: Specification for information security management systems*.

BS EN ISO 14001:1996, *Environmental management systems — Specification with guidance for use*.

BS ISO/IEC TR 13335-3:1998, *Guidelines for the Management of IT Security — Part 3: Techniques for the management of IT security*.

BS ISO/IEC TR 13335-4:2000, *Guidelines for the Management of IT Security — Part 4: Selection of safeguards*.

ISO/IEC Guide 62:1996, *General requirements for bodies operating assessment and certification / registration of quality systems*.

Other publications

[1] OECD. *OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security*. Paris: OECD, July 2002. www.oecd.org

BSI — British Standards Institution

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

Revisions

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

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

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

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at <http://www.bsi-global.com>.

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

Information on standards

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

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

Information regarding online access to British Standards via British Standards Online can be found at <http://www.bsi-global.com/bsonline>.

Further information about BSI is available on the BSI website at <http://www.bsi-global.com>.

Copyright

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI.

This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained.

Details and advice can be obtained from the Copyright & Licensing Manager. Tel: +44 (0)20 8996 7070. Fax: +44 (0)20 8996 7553. Email: copyright@bsi-global.com.

BSI
389 Chiswick High Road
London
W4 4AL