

Information security management —

Part 2: Specification for information security management systems

ICS 35.020; 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

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:

- Association of British Insurers
- British Computer Society
- British Telecommunications plc
- The Business Continuity Institute
- Department of Trade and Industry (Information Security Policy Group)
- Det Norske Veritas Quality Assurance
- HMG Protective Security Authority
- HSBC
- Indicii Salus
- Institute of Chartered Accountants in England and Wales
- Institute of Internal Auditors
- KPMG plc
- L3 Network Security
- Lloyds TSB
- Logica UK
- Marks and Spencer plc
- Nationwide Building Society
- PCSL
- Racal Network Services
- RKP Associates
- Shell International Petroleum Co Ltd
- Unilever plc
- Whitbread plc
- XiSEC Consultants Ltd/AEXIS Consultants

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 May 1999

© BSI 02-2001

First published as Part 2 February 1998

The following BSI references relate to work on this standard: Committee reference BDD/2

ISBN 0 580 28280 5

Amendments issued since publication

Amd. No.	Date	Comments
13087	February 2001	Indicated by a sideline.

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
1 Scope	1
2 Terms and definitions	1
3 Information security management system requirements	1
3.1 General	1
3.2 Establishing a management framework	1
3.3 Implementation	1
3.4 Documentation	1
3.5 Document control	1
3.6 Records	2
4 Detailed controls	2
4.1 Security policy	2
4.2 Organizational security	3
4.3 Asset classification and control	3
4.4 Personnel security	3
4.5 Physical and environmental security	4
4.6 Communications and operations management	5
4.7 Access control	6
4.8 Systems development and maintenance	7
4.9 Business continuity management	8
4.10 Compliance	8
Figure 1 — Establishing a management framework	2
Annex A (informative) Changes to internal numbering	10
Bibliography	11

Foreword

This part of BS 7799 has been prepared by BDD/2, Information security management. It supersedes BS 7799-2:1998, which is withdrawn.

BS 7799 is issued in two parts:

- *Part 1: Code of practice for information security management*¹⁾;
- *Part 2: Specification for information security management systems.*

This new edition of BS 7799-2 is required because the numbering system, the control objectives, and the controls given in clause 4 of this part of BS 7799 are directly derived from and aligned with those listed in clauses 3 to 12 of BS 7799-1¹⁾ which has been revised. No other changes have been introduced.

As a new edition, this does not represent a full review or revision of the standard, which will be undertaken in due course.

It forms the basis for an assessment of the information security management system (ISMS) of the whole, or part, of an organization. It may be used as a basis for a formal certification scheme.

This specification is based on BS 7799-1, *Information security management — Part 1: Code of practice for information security management*¹⁾, which provides guidance on best practice in support of the requirements of this specification. However, the list of control objectives and controls in clause 4 of this part of BS 7799 is not exhaustive and an organization may 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. Organizations need to undertake a risk assessment to identify the most appropriate control objectives and controls to be implemented which are applicable to their own needs. Once identified, these need to be recorded in a statement of applicability. The statement of applicability needs to be accessible to managers, personnel and any third party (e.g. auditors, certifiers, etc.) authorized to have access to it. The control objectives and controls recorded in the statement of applicability, together with the policy and procedure documents and all other relevant records, are known as the organization's ISMS.

The requirements given in clause 4 of this part of BS 7799 are deliberately general in their nature. It is expected that organizations seeking certification will adopt those elements of best practice given in part 1¹⁾ that the risk assessment demonstrates are most appropriate to their needs. Any conditions associated with a certification scheme will be issued separately under the authority of the scheme owner and do not fall within the scope of this standard. To be certifiable against this British Standard the ISMS will be implemented and maintained to the satisfaction of the third party certification body.

It has been assumed in the drafting of this British Standard that the execution of its provisions is entrusted to appropriately qualified and experienced people.

Annex A is informative and contains a table showing the relationship between the sections of the 1998 edition and the clauses of the 1999 edition.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of 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 11 and a back cover.

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

Sidelining in this document indicates the most recent changes by amendment.

¹⁾ Part 1 of BS 7799 has now been adopted by ISO/IEC and is currently available as BS ISO/IEC 17799:2000. BS ISO/IEC 17799:2000 contains a national annex which enables users to quickly identify changes between it and BS 7799-1:1999.

1 Scope

This part of BS 7799 specifies requirements for establishing, implementing and documenting information security management systems (ISMSs). It specifies requirements for security controls to be implemented according to the needs of individual organizations.

NOTE BS ISO/IEC 17799 gives recommendations for best practice in support of the requirements of this specification. The control objectives and controls given in clause 4 of this part of BS 7799 are derived from and aligned with the objectives and controls listed in BS ISO/IEC 17799:2000.

2 Terms and definitions

For the purposes of this part of BS 7799, the definitions given in BS ISO/IEC 17799 apply, together with the following.

2.1

statement of applicability

critique of the objectives and controls applicable to the needs of the organization

3 Information security management system requirements

3.1 General

The organization shall establish and maintain a documented ISMS. This shall address the assets to be protected, the organization's approach to risk management, the control objectives and controls, and the degree of assurance required.

3.2 Establishing a management framework

The following steps shall be undertaken to identify and document the control objectives and controls (see Figure 1).

- The information security policy shall be defined.
- The scope of the information security management system shall be defined. The boundaries shall be defined in terms of the characteristics of the organization, its location, assets and technology.
- An appropriate risk assessment shall be undertaken. The risk assessment shall identify the threats to assets, vulnerabilities and impacts on the organization and shall determine the degree of risk.
- The areas of risk to be managed shall be identified based on the organization's information security policy and the degree of assurance required.
- Appropriate control objectives and controls shall be selected from clause 4 for implementation by the organization, and the selection shall be justified.

NOTE Guidance on the selection of control objectives and controls can be found in BS ISO/IEC 17799. The control objectives and controls listed in clause 4 of this part of BS 7799 are not exhaustive and additional controls may also be selected.

- A statement of applicability shall be prepared. The selected control objectives and controls, and the reasons for their selection shall be documented in the statement of applicability. This statement shall also record the exclusion of any controls listed in clause 4.

These steps shall be reviewed at appropriately defined intervals as required.

3.3 Implementation

The selected control objectives and controls shall be implemented effectively by the organization. The effectiveness of the procedures adopted to implement the controls shall be verified by reviews in accordance with 4.10.2.

NOTE Attention is drawn to the recommendations given in BS ISO/IEC 17799.

3.4 Documentation

The ISMS documentation shall consist of the following information:

- evidence of the actions undertaken as specified in 3.2;
- a summary of the management framework including the information security policy and the control objectives and implemented controls given in the statement of applicability;
- the procedures adopted to implement the controls as specified in 3.3. These shall describe responsibilities and relevant actions;
- the procedures covering the management and operation of the ISMS. These shall describe responsibilities and relevant actions.

NOTE The documents listed in 3.4b) and c) may be conveniently placed together in a security policy manual.

3.5 Document control

The organization shall establish and maintain procedures for controlling all documentation required under 3.4 to ensure that the documentation is:

- readily available;
- periodically reviewed and revised as necessary in line with the organization's security policy;
- maintained under version control and made available at all locations where operations essential to the effective functioning of the ISMS are performed;
- promptly withdrawn when obsolete;
- identified and retained when obsolete and required for legal or knowledge preservation purposes, or both.

Documentation shall be legible, dated (together with dates of revision) and readily identifiable, maintained in an orderly manner and retained for a specified period. Procedures and responsibilities shall be established and maintained for the creation and modification of the various types of document.

NOTE Documents may be in any medium, such as hard copy or electronic media.