

Information security management

Part 2. Specification for information security management systems

ICS 35.020; 35.110

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents



Document Sharing Hub

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the DISC Board to Technical Committee BDD/2, upon which the following bodies were represented:

- Association of British Industries
- British Computer Society
- British Telecommunications plc
- Department of Trade and Industry (IT Standards Unit)
- Det Norske Veritas Quality Assurance
- Lloyds TSB
- Logica UK
- Marks & Spencer plc
- Midland Bank plc
- Nationwide Building Society
- Prudential Assurance Co. Ltd.
- Unilever
- Xisec Consultants

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Board and comes into effect on 15 February 1998

© BSI 1998

The following BSI references relate to the work on this standard:
Committee reference BDD/2
Draft for comment 97/600130 DC

ISBN 0 580 28995 8

Amendments issued since publication

Amd. No.	Date	Text affected

Contents

	Page
Committees responsible	Inside front cover
Foreword	ii
Section 1. General	
1.1 Scope	1
1.2 Definitions	1
Section 2. Information security management system requirements	
2.1 General	2
2.2 Establishing a management framework	2
2.3 Implementation	2
2.4 Documentation	2
2.5 Document control	2
2.6 Records	2
Section 3. Detailed controls	
3.1 Information security policy	4
3.2 Security organization	4
3.3 Assets classification and control	4
3.4 Personnel security	4
3.5 Physical and environmental security	5
3.6 Computer and network management	5
3.7 System access control	6
3.8 Systems development and maintenance	7
3.9 Business continuity planning	8
3.10 Compliance	8
Figure	
1 Establishing a management framework	3
List of references	Inside back cover

Foreword

This Part of BS 7799 has been prepared by BDD/2, Information Security Management. 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 : Part 1 *Code of Practice for information security management systems*, which provides guidance on best practice in support of the requirements of this specification. The numbering system, the control objectives and the controls given in section 3 of this Part of BS 7799 are directly derived from and aligned with those listed in annex A of Part 1. However, the list of control objectives and controls in section 3 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 information security management system.

The requirements given in section 3 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 1 that the risk analysis 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.

Part 1 of BS 7799 refers to 10 key controls. These controls are included but not emphasized in this specification. It has been assumed that the ISMS includes the 10 key controls where the risk assessment demonstrates that they are applicable.

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.

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 8, an inside back cover and a back cover.

Section 1. General

1.1 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.

Part 1 gives recommendations for best practice in support of the requirements of this specification. The control objectives and controls given in section 3 of this Part of BS 7799 are derived from and aligned with the objectives and controls listed in annex A of Part 1 : 1995.

1.2 Definitions

For the purposes of this Part of BS 7799, the definitions given in Part 1 of BS 7799 apply, together with the following.

1.2.1 statement of applicability

Critique of the objectives and controls applicable to the needs of the organization.