AS/NZS 4444.2:2000
BS 7799.2:1999
(Incorporating Amendment No. 1)

Information security management

Part 2: Specification for information security management systems

Standards Australia
STANDARDS NEW ZEALAND
Paerewa Aotearoa

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT/12, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 7 January 2000 and on behalf of the Council of Standards New Zealand on 25 February 2000. It was published on 31 March 2000.

The following interests are represented on Committee IT/12:

Attorney General's Department
Australia Post
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Customs Service, Commonwealth
Australian Electrical and Electronic Manufacturers Association
Australian Information Industry Association
Consumers Federation of Australia
Department of Defence, Australia

A1

Government Communications Security Bureau, New Zealand
New Zealand Defence Force
NSW Police Service
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

A1 Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Australia web site at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia International or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 99448.

(Incorporating Amendment No.1)

Information security management

Part 2: Specification for information security management systems

AS/NZS 4444.2:2000
BS 7799.2:1999

Jointly published by Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001
and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 3284 4

This page left intentionally blank

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT/12, Information Systems, Security and Identification Technology.

This Standard incorporates Amendment 1 (October 2000). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

AS/NZS 4444/BS 7799, *Information security management*, is issued in two parts as follows:

Part 1: *Code of practice for information security management*

Part 2: *Specification for information security management systems*

AS/NZS 4444.2:2000 is identical to BS 7799—2:1999. It has been reviewed by Standards Australia and Standards New Zealand.

This Standard 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.

AS/NZS 4444.2/BS 7799.2 (this Standard) should be read in conjunction with AS/NZS 4444.1/BS 7799.1, *Information security management*, Part 1: *Code of practice for information security management*, which provides guidance on best practice in support of the requirements of this Standard; however, the list of control objectives and controls in Clause 4 of this part of AS/NZS 4444/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. It should be noted that in Australia, the use of authentication and encryption technology and systems is encouraged along with procedures that allow users to recover secured data in the event of the unavailability of decryption keys. It should also be noted that a range of electronic authentication techniques are emerging (of which digital signatures is a special case) and that techniques other than digital signatures may sometimes be the best way to achieve risk management objectives. 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 AS/NZS 4444/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 which the risk assessment demonstrates are most appropriate to their needs. Any conditions associated with a certification scheme are not within the scope of this Standard. They should be issued separately under the authority of the scheme owner. To be certifiable against this Australian/New Zealand Standard the ISMS should be implemented and maintained to the satisfaction of the third party certification body.

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

Compliance with this Australia/New Zealand Standard does not confer immunity from legal obligations.

Contents

1 Scope 1

2 Terms and definitions 2
2.1 Statement of applicability 2

3 Information security management system requirements 3
3.1 General 3
3.2 Establishing a management framework 3
3.3 Implementation 4
3.4 Documentation 4
3.5 Document control 4
3.6 Records 5

4 Detailed controls 6
4.1 Security policy 6
4.2 Security organization 6
4.3 Asset classification and control 8
4.4 Personnel security 8
4.5 Physical and environmental security 10
4.6 Communications and operations management 11
4.7 Access control 14
4.8 Systems development and maintenance 18
4.9 Business continuity management 20
4.10 Compliance 20

This page left intentionally blank

1 Scope

This Standard 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: AS/NZS 4444.1/BS 7799.1 gives recommendations for best practice in support of the requirements of this specification. The control objectives and controls given in Clause 4 of this Standard are derived from and aligned with the objectives and controls listed in AS/NZS 4444.1/BS 7799.1.