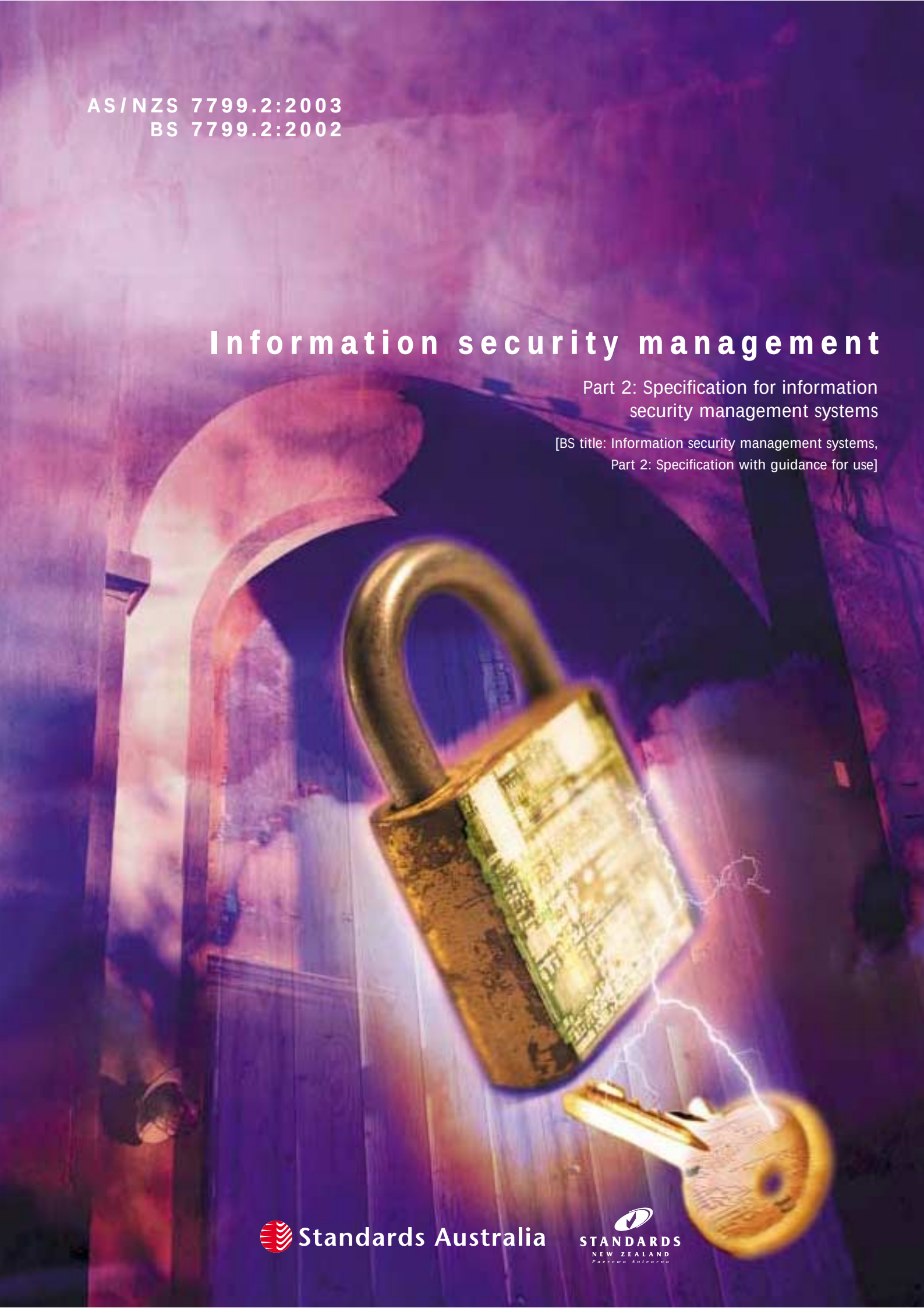
AS/NZS 7799.2:2003
BS 7799.2:2002

Information security management

Part 2: Specification for information security management systems

[BS title: Information security management systems, Part 2: Specification with guidance for use]



Standards Australia

STANDARDS NEW ZEALAND
Paerewa Aotearoa

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 31 December 2002 and on behalf of the Council of Standards New Zealand on 13 December 2002. It was published on 11 February 2003.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Australian Information Industry Association
Certification Forum of Australia
Department of Defence, Australia
Department of Social Welfare, New Zealand
Government Communications Security Bureau, New Zealand
Internet Industry Association
NSW Police Service
New Zealand Defence Force
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 Standards may also be withdrawn.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.

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 02470.

Information security management

Part 2: Specification for information security management systems

AS/NZS 7799.2:2003
BS 7799.2:2002

Originated as part of AS/NZS 4444:1996.
Previous edition AS/NZS 7799.2:2000.
Second edition AS/NZS 7799.2:2003.

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 5011 7

This page left intentionally blank

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology. It supersedes AS/NZS 7799.2:2000, *Information security management,* Part 2: *Specification for information security management systems*.

This Standard is identical with BS 7799.2:2002, *Information security management systems,* Part 2: *Specification with guidance for use* and has been reviewed by Standards Australia and Standards New Zealand. This standard is an adoption of BS 7799.2:2002 and is implemented with the permission of British Standards Publishing Ltd.

This Standard is to be read in conjunction with AS/NZS ISO/IEC 17799:2001, *Information technology—Code of practice for information security management*.

This new edition has been produced to provide a management system specification that is consistent with other management system standards such as ISO 9001 and ISO 14001. This new edition also introduces a Plan-Do-Check-Act (PDCA) process 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 also embraces the principles as set out in the OECD guidance (2002) governing the security of information systems and networks. In particular, the Standard gives a robust model for implementing the last four principles in those guidelines on risk assessment, safeguards, security management and reassessment.

The control objectives and controls referred to in this edition are directly derived from and aligned with those listed in AS/NZS ISO/IEC 17799:2001. The list of control objectives and controls of this Standard are not exhaustive and an organization may consider that additional control objectives and controls are necessary. The control objectives and controls implemented within an information security management system should be selected as a result of a business risk management process as relevant to the business.

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.

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 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 requirements of this Standard are deliberately general in nature. It is expected that organizations seeking certification of an Information Security Management System (ISMS) will adopt relevant elements of best practice given in AS/NZS ISO/IEC 17799:2001.

Any conditions associated with certification are not within the scope of this standard. They should be issued separately under the authority of the certification scheme owner. To be certifiable against this Standard, the organization's ISMS should be implemented and maintained to the satisfaction of the certification body.

It has been assumed in the drafting of this Standard that the execution of its provisions is entrusted to appropriately qualified and experienced people. Compliance with this Standard does not confer immunity from legal obligations.

Annex A is normative and contains the control objectives and controls from AS/NZS ISO/IEC 17799:2001. Annex B is informative and provides guidance on the use and interpretation of this standard. Annex C is informative and shows the correspondence between the clauses of this standard, ISO 9001:2000 and ISO 14001:1996. Annex D is informative and shows the correspondence between section numbers in the 2000 edition of AS/NZS 7799.2 and the clause numbers in this edition.

Contents

FIGURES

TABLES

Introduction

General

This 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 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.

Process approach

This 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.

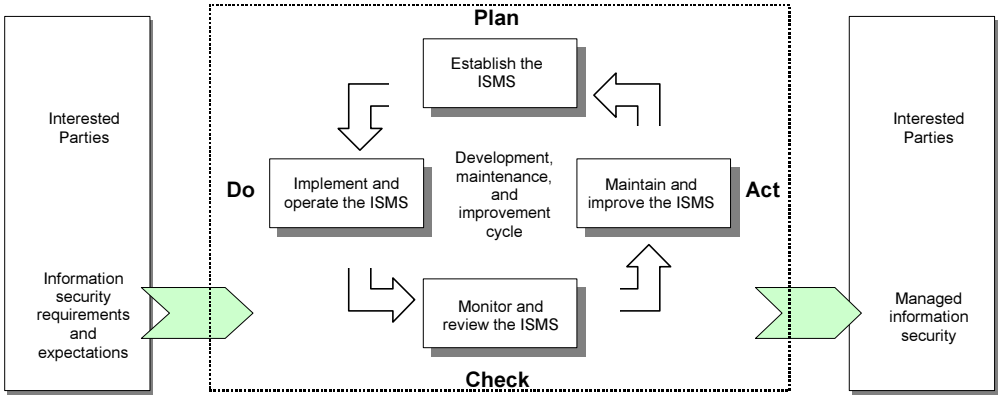


Figure 1 — PDCA model applied to ISMS processes

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.

Compatibility with other management systems

This standard is aligned with ISO 001:2000 and ISO 4001:1996 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 standard, ISO 9001:2000 and ISO 14001:1996.

This 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 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.