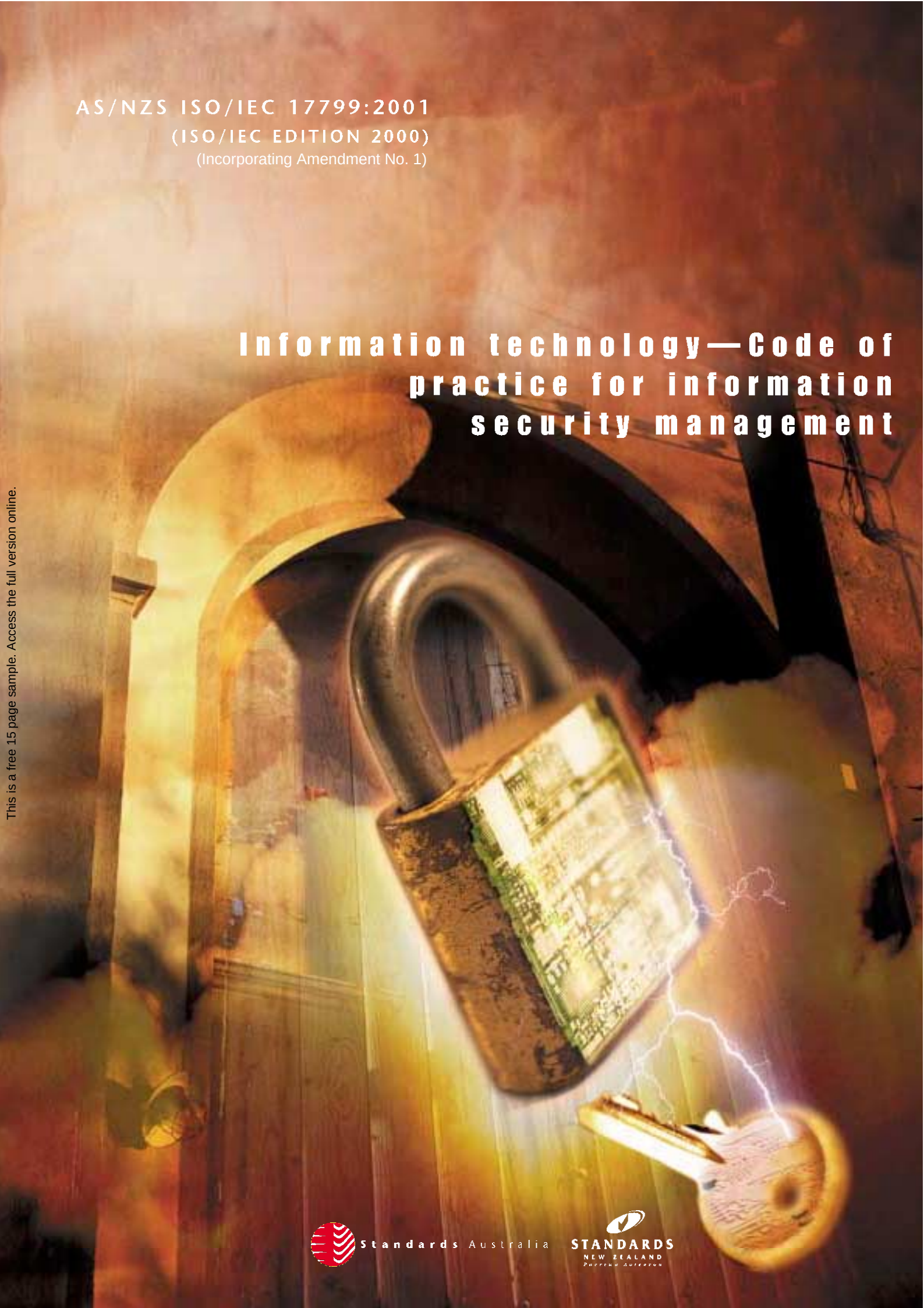
AS/NZS ISO/IEC 17799:2001

(ISO/IEC EDITION 2000)

(Incorporating Amendment No. 1)

Information technology—Code of practice for information security management



Standards Australia

STANDARDS NEW ZEALAND

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 04 May 2001 and on behalf of the Council of Standards New Zealand on 4 May 2001. It was published on 8 June 2001.

The following are represented on Committee IT-012:

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
Department of Social Welfare, New Zealand
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 Standards may also be withdrawn.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.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop 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 00408.

Information technology— Code of practice for information security management

AS/NZS ISO/IEC 17799:2001
(Incorporating Amendment No. 1)

Originated as part of AS/NZS 4444:1996.
Previous edition AS/NZS 4444.1:1999.
Jointly revised and redesignated AS/NZS ISO/IEC 17799:2001.
Reissued and incorporating Amdt No. 1 (March 2004)

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 3876 1

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology and supersedes AS/NZS 4444.1:1999, *Information security management*, Part 1: *Code of practice for information security management*.

This Standard incorporates Amendment No. 1 (March 2004). 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.

It is identical with ISO/IEC 17799:2000, *Information technology—Code of practice for information security management* and differs in only very minor editorial details from AS/NZS 4444.1:1999. However the Standard number has been changed to that of the international Standard (ISO/IEC 17799) to minimize any confusion when it is used by organizations internationally.

The objective of this Standard is to give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.

This Standard is complementary to AS/NZS 4444.2:2000, *Information security management*, Part 2: *Specification for information security management systems* (redesignated in Amendment 2 as AS/NZS 7799.2:2000) and HB 231:2000, *Information security risk management guidelines*.

As this Standard is reproduced from an International Standard, the following applies:

(a) In the source text ‘this International Standard’ should read ‘this Australian/New Zealand Standard’.

(b) A full point should be substituted for a comma when referring to a decimal marker.

Information is a vital asset in any organization. The protection and security of information is of prime importance to many aspects of an organization’s business. It is therefore important that an organization implements a suitable set of controls and procedures to achieve information security and manages them to retain that level of security once it is achieved.

This Standard is intended for use by managers and employees who are responsible for initiating, implementing and maintaining information security within their organization and it may be considered as a basis for developing organizational security standards.

A comprehensive set of controls comprising the best information security practices currently in use is provided in this Standard. This guidance is intended to be as comprehensive as possible. It is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce and can therefore be applied by large, medium and small organizations.

With increasing electronic networking between organizations there is a clear benefit in having a common reference document for information security management. It enables mutual trust to be established between networked information systems and trading partners and provides a basis for the management of these systems between users and service providers.

Not all the controls described in this Standard will be relevant to every situation. It cannot take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization. Consequently this Standard might need to be supplemented by further guidance. It can be used as a basis from which, for example, a corporate policy or an inter-company trading agreement can be developed.

The guidance and recommendations provided throughout this Standard should not be quoted as if they were specifications. In particular, care should be taken to ensure that claims of compliance are not misleading.

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

Contents

A1

Introduction

What is information security?

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is characterized here as the preservation of:

(a) confidentiality: ensuring that information is accessible only to those authorized to have access;

(b) integrity: safeguarding the accuracy and completeness of information and processing methods;

(c) availability: ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

Why information security is needed

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information may be essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image.

Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organization. It may also require participation from suppliers, customers or shareholders. Specialist advice from outside organizations may also be needed.

Information security controls are considerably cheaper and more effective if incorporated at the requirements specification and design stage.

A1

How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources.

The first source is derived from assessing risks to the organization. Through risk assessment threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

The second source is the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy.

The third source is the particular set of principles, objectives and requirements for information processing that an organization has developed to support its operations.

Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. Risk assessment techniques can be applied to the whole organization, or only parts of it, as well as to individual information systems, specific system components or services where this is practicable, realistic and helpful.

Risk assessment is systematic consideration of:

(a) the business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;

(b) the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

The results of this assessment will help guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

It is important to carry out periodic reviews of security risks and implemented controls to:

(i) take account of changes to business requirements and priorities;

(ii) consider new threats and vulnerabilities;

(iii) confirm that controls remain effective and appropriate.

Reviews should be performed at different levels of depth depending on the results of previous assessments and the changing levels of risk that management is prepared to accept. Risk assessments are often carried out first at a high level, as a means of prioritizing resources in areas of high risk, and then at a more detailed level, to address specific risks.

A1

Selecting controls

Once security requirements have been identified, controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this document or from other control sets, or new controls can be designed to meet specific needs as appropriate. There are many different ways of managing risks and this document provides examples of common approaches. However, it is necessary to recognize that some of the controls are not applicable to every information system or environment, and might not be practicable for all organizations. As an example, 8.1.4 describes how duties may be segregated to prevent fraud and error. It may not be possible for smaller organizations to segregate all duties and other ways of achieving the same control objective may be necessary. As another example, 9.7 and 12.1 describe how system use can be monitored and evidence collected. The described controls e.g. event logging might conflict with applicable legislation, such as privacy protection for customers or in the workplace.

Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors such as loss of reputation should also be taken into account.

Some of the controls in this document can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading “Information security starting point”.

Information security starting point

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security.

Controls considered to be essential to an organization from a legislative point of view include:

(a) data protection and privacy of personal information (see 12.1.4).

(b) safeguarding of organizational records (see 12.1.3);

(c) intellectual property rights (see 12.1.2);

Controls considered to be common best practice for information security include:

(i) information security policy document (see 3.1);

(ii) allocation of information security responsibilities (see 4.1.3);

(iii) information security education and training (see 6.2.1);

(iv) reporting security incidents (see 6.3.1);

(v) business continuity management (see 11.1).

These controls apply to most organizations and in most environments. It should be noted that although all controls in this document are important, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

A1

Critical success factors

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

(a) security policy, objectives and activities that reflect business objectives;

(b) an approach to implementing security that is consistent with the organizational culture;

(c) visible support and commitment from management;

(d) a good understanding of the security requirements, risk assessment and risk management;

(e) effective marketing of security to all managers and employees;

(f) distribution of guidance on information security policy and standards to all employees and contractors;

(g) providing appropriate training and education;

(h) a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidance. Not all of the guidance and controls in this code of practice may be applicable. Furthermore, additional controls not included in this document may be required. When this happens it may be useful to retain cross-references which will facilitate compliance checking by auditors and business partners.

NOTES

Information technology — Code of practice for information security management

1 Scope

This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings. Recommendations from this standard should be selected and used in accordance with applicable laws and regulations.

2 Terms and definitions

For the purposes of this document, the following definitions apply.

2.1 Information security

Preservation of confidentiality, integrity and availability of information.

- **Confidentiality**
  Ensuring that information is accessible only to those authorized to have access.

- **Integrity**
  Safeguarding the accuracy and completeness of information and processing methods.

- **Availability**
  Ensuring that authorized users have access to information and associated assets when required.

2.2 Risk assessment

Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

2.3 Risk management

Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost.

3 Security policy

3.1 Information security policy

Objective: To provide management direction and support for information security.
Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

3.1.1 Information security policy document

A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security. As a minimum, the following guidance should be included:

AS/NZS ISO/IEC 17799:2001 Information technology - Code of practice for information security management