STANDARDS Australia

AS/NZS ISO/IEC 17799:2006

Information technology — Security techniques — Code of practice for information security management

STANDARD

AS/NZS

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 23 May 2006 and on behalf of the Council of Standards New Zealand on 16 June 2006.
This Standard was published on 6 July 2006.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Department of Defence
Department of Social Welfare, NZ
Government Communications Security Bureau, NZ
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 Standards may also be withdrawn.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 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 or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 06092.

Australian/New Zealand Standard™

Information technology—Security techniques—Code of practice for information security management

Originated as part of AS/NZS 4444:1996.
Previous edition AS/NZS ISO/IEC 17799:2001.
Second edition 2006.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 7492 X

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology to supersede AS/NZS ISO/IEC 17799:2001.

This Standard is identical with and has been reproduced from ISO/IEC 17799:2005.

The objective of this Standard is to provide a practical guideline for developing organizational security, standards and effective security management practices and to help build confidence in inter-organizational activities.

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

(a) Its number appears on the cover and title page while the international standard number appears only on the cover

(b) In the source text ‘this International Standard’ should read ‘Australian Standard’.

(c) A full point substitutes for a comma when referring to a decimal marker.

CONTENTS

Page

Page

Page

Page

INTRODUCTION

0.1 What is information security?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see also OECD Guidelines for the Security of Information Systems and Networks).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by 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 the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

0.2 Why information security is needed?

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

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. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also 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 requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties. Specialist advice from outside organizations may also be needed.

0.3 How to establish security requirements

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

1. One source is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.

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

0.4 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.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

More information about the assessment of security risks can be found in clause 4.1 "Assessing security risks".

0.5 Selecting controls

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate. The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations.

Some of the controls in this standard 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".

More information about selecting controls and other risk treatment options can be found in clause 4.2 "Treating security risks".

0.6 Information security starting point

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

Controls considered to be essential to an organization from a legislative point of view include, depending on applicable legislation:

a) data protection and privacy of personal information (see 15.1.4);

b) protection of organizational records (see 15.1.3);

c) intellectual property rights (see 15.1.2).

Controls considered to be common practice for information security include:

a) information security policy document (see 5.1.1);

b) allocation of information security responsibilities (see 6.1.3);

c) information security awareness, education, and training (see 8.2.2);

d) correct processing in applications (see 12.2);

e) technical vulnerability management (see 12.6);

f) business continuity management (see 14);

g) management of information security incidents and improvements (see 13.2).

These controls apply to most organizations and in most environments.

It should be noted that although all controls in this standard are important and should be considered, 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.

0.7 Critical success factors

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

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

b) an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;

c) visible support and commitment from all levels of management;

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

e) effective marketing of information security to all managers, employees, and other parties to achieve awareness;

f) distribution of guidance on information security policy and standards to all managers, employees and other parties;

g) provision to fund information security management activities;

h) providing appropriate awareness, training, and education;

i) establishing an effective information security incident management process;

j) implementation of a measurement [1] system that is used to evaluate performance in information security management and feedback suggestions for improvement.

[1] Note that information security measurements are outside of the scope of this standard.

0.8 Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology — Security techniques — Code of practice for information security management

1 Scope

This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

The control objectives and controls of this International Standard are intended to be implemented to meet the requirements identified by a risk assessment. This International Standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

2 Terms and definitions

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

2.1

asset
anything that has value to the organization
[ISO/IEC 13335-1:2004]

2.2

control
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
NOTE Control is also used as a synonym for safeguard or countermeasure.

2.3

guideline
a description that clarifies what should be done and how, to achieve the objectives set out in policies
[ISO/IEC 13335-1:2004]

2.4

information processing facilities
any information processing system, service or infrastructure, or the physical locations housing them

2.5

information security
preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved

2.6

information security event
an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
[ISO/IEC TR 18044:2004]

AS/NZS ISO/IEC 17799:2006 Information technology - Security techniques - Code of practice for information security management