

STANDARDS
Australia



A1 | AS/NZS ISO/IEC 27002:2006
(Incorporating Amendment No. 1)

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



STANDARD

AS/NZS



This is a preview. [Click here to purchase the full publication.](#)

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 Standards may also be withdrawn.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.
Reissued incorporating Amendment No. 1 (August 2008).

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

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

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 incorporates Amendment No. 1 (August 2008). 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.

A1

This Standard is identical with and has been reproduced from ISO/IEC 27002:2005. ISO/IEC 27002:2005 comprises ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor.1:2007. Its technical content is identical to that of ISO/IEC 17799:2005. ISO/IEC 17799:2005/Cor.1:2007 changes the reference number of the standard from 17799 to 27002.

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

1	SCOPE	1
2	TERMS AND DEFINITIONS	1
3	STRUCTURE OF THIS STANDARD.....	4
3.1	CLAUSES	4
3.2	MAIN SECURITY CATEGORIES	4
4	RISK ASSESSMENT AND TREATMENT	5
4.1	ASSESSING SECURITY RISKS	5
4.2	TREATING SECURITY RISKS.....	5
5	SECURITY POLICY	7
5.1	INFORMATION SECURITY POLICY	7
5.1.1	<i>Information security policy document</i>	<i>7</i>
5.1.2	<i>Review of the information security policy.....</i>	<i>8</i>
6	ORGANIZATION OF INFORMATION SECURITY.....	9
6.1	INTERNAL ORGANIZATION	9
6.1.1	<i>Management commitment to information security.....</i>	<i>9</i>
6.1.2	<i>Information security co-ordination.....</i>	<i>10</i>
6.1.3	<i>Allocation of information security responsibilities.....</i>	<i>10</i>
6.1.4	<i>Authorization process for information processing facilities.....</i>	<i>11</i>
6.1.5	<i>Confidentiality agreements.....</i>	<i>11</i>
6.1.6	<i>Contact with authorities</i>	<i>12</i>
6.1.7	<i>Contact with special interest groups</i>	<i>12</i>
6.1.8	<i>Independent review of information security</i>	<i>13</i>
6.2	EXTERNAL PARTIES	14
6.2.1	<i>Identification of risks related to external parties.....</i>	<i>14</i>
6.2.2	<i>Addressing security when dealing with customers</i>	<i>15</i>
6.2.3	<i>Addressing security in third party agreements</i>	<i>16</i>
7	ASSET MANAGEMENT.....	19
7.1	RESPONSIBILITY FOR ASSETS.....	19
7.1.1	<i>Inventory of assets</i>	<i>19</i>
7.1.2	<i>Ownership of assets</i>	<i>20</i>
7.1.3	<i>Acceptable use of assets.....</i>	<i>20</i>
7.2	INFORMATION CLASSIFICATION.....	21
7.2.1	<i>Classification guidelines.....</i>	<i>21</i>
7.2.2	<i>Information labeling and handling.....</i>	<i>21</i>
8	HUMAN RESOURCES SECURITY	23
8.1	PRIOR TO EMPLOYMENT	23
8.1.1	<i>Roles and responsibilities</i>	<i>23</i>

8.1.2	Screening	23
8.1.3	Terms and conditions of employment	24
8.2	DURING EMPLOYMENT	25
8.2.1	Management responsibilities	25
8.2.2	Information security awareness, education, and training	26
8.2.3	Disciplinary process	26
8.3	TERMINATION OR CHANGE OF EMPLOYMENT	27
8.3.1	Termination responsibilities	27
8.3.2	Return of assets	27
8.3.3	Removal of access rights	28
9	PHYSICAL AND ENVIRONMENTAL SECURITY	29
9.1	SECURE AREAS	29
9.1.1	Physical security perimeter	29
9.1.2	Physical entry controls	30
9.1.3	Securing offices, rooms, and facilities	30
9.1.4	Protecting against external and environmental threats	31
9.1.5	Working in secure areas	31
9.1.6	Public access, delivery, and loading areas	32
9.2	EQUIPMENT SECURITY	32
9.2.1	Equipment siting and protection	32
9.2.2	Supporting utilities	33
9.2.3	Cabling security	34
9.2.4	Equipment maintenance	34
9.2.5	Security of equipment off-premises	35
9.2.6	Secure disposal or re-use of equipment	35
9.2.7	Removal of property	36
10	COMMUNICATIONS AND OPERATIONS MANAGEMENT	37
10.1	OPERATIONAL PROCEDURES AND RESPONSIBILITIES	37
10.1.1	Documented operating procedures	37
10.1.2	Change management	37
10.1.3	Segregation of duties	38
10.1.4	Separation of development, test, and operational facilities	38
10.2	THIRD PARTY SERVICE DELIVERY MANAGEMENT	39
10.2.1	Service delivery	39
10.2.2	Monitoring and review of third party services	40
10.2.3	Managing changes to third party services	40
10.3	SYSTEM PLANNING AND ACCEPTANCE	41
10.3.1	Capacity management	41
10.3.2	System acceptance	41
10.4	PROTECTION AGAINST MALICIOUS AND MOBILE CODE	42
10.4.1	Controls against malicious code	42
10.4.2	Controls against mobile code	43
10.5	BACK-UP	44
10.5.1	Information back-up	44
10.6	NETWORK SECURITY MANAGEMENT	45
10.6.1	Network controls	45
10.6.2	Security of network services	46
10.7	MEDIA HANDLING	46
10.7.1	Management of removable media	46
10.7.2	Disposal of media	47
10.7.3	Information handling procedures	47
10.7.4	Security of system documentation	48
10.8	EXCHANGE OF INFORMATION	48
10.8.1	Information exchange policies and procedures	49
10.8.2	Exchange agreements	50
10.8.3	Physical media in transit	51
10.8.4	Electronic messaging	52
10.8.5	Business information systems	52

	Page
10.9 ELECTRONIC COMMERCE SERVICES	53
10.9.1 <i>Electronic commerce</i>	53
10.9.2 <i>On-Line Transactions</i>	54
10.9.3 <i>Publicly available information</i>	55
10.10 MONITORING	55
10.10.1 <i>Audit logging</i>	55
10.10.2 <i>Monitoring system use</i>	56
10.10.3 <i>Protection of log information</i>	57
10.10.4 <i>Administrator and operator logs</i>	58
10.10.5 <i>Fault logging</i>	58
10.10.6 <i>Clock synchronization</i>	58
11 ACCESS CONTROL	60
11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL	60
11.1.1 <i>Access control policy</i>	60
11.2 USER ACCESS MANAGEMENT	61
11.2.1 <i>User registration</i>	61
11.2.2 <i>Privilege management</i>	62
11.2.3 <i>User password management</i>	62
11.2.4 <i>Review of user access rights</i>	63
11.3 USER RESPONSIBILITIES	63
11.3.1 <i>Password use</i>	64
11.3.2 <i>Unattended user equipment</i>	64
11.3.3 <i>Clear desk and clear screen policy</i>	65
11.4 NETWORK ACCESS CONTROL	65
11.4.1 <i>Policy on use of network services</i>	66
11.4.2 <i>User authentication for external connections</i>	66
11.4.3 <i>Equipment identification in networks</i>	67
11.4.4 <i>Remote diagnostic and configuration port protection</i>	67
11.4.5 <i>Segregation in networks</i>	68
11.4.6 <i>Network connection control</i>	68
11.4.7 <i>Network routing control</i>	69
11.5 OPERATING SYSTEM ACCESS CONTROL	69
11.5.1 <i>Secure log-on procedures</i>	69
11.5.2 <i>User identification and authentication</i>	70
11.5.3 <i>Password management system</i>	71
11.5.4 <i>Use of system utilities</i>	72
11.5.5 <i>Session time-out</i>	72
11.5.6 <i>Limitation of connection time</i>	72
11.6 APPLICATION AND INFORMATION ACCESS CONTROL	73
11.6.1 <i>Information access restriction</i>	73
11.6.2 <i>Sensitive system isolation</i>	74
11.7 MOBILE COMPUTING AND TELEWORKING	74
11.7.1 <i>Mobile computing and communications</i>	74
11.7.2 <i>Teleworking</i>	75
12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	77
12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS	77
12.1.1 <i>Security requirements analysis and specification</i>	77
12.2 CORRECT PROCESSING IN APPLICATIONS	78
12.2.1 <i>Input data validation</i>	78
12.2.2 <i>Control of internal processing</i>	78
12.2.3 <i>Message integrity</i>	79
12.2.4 <i>Output data validation</i>	79
12.3 CRYPTOGRAPHIC CONTROLS	80
12.3.1 <i>Policy on the use of cryptographic controls</i>	80
12.3.2 <i>Key management</i>	81
12.4 SECURITY OF SYSTEM FILES	83
12.4.1 <i>Control of operational software</i>	83
12.4.2 <i>Protection of system test data</i>	84

	Page
12.4.3 Access control to program source code.....	84
12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	85
12.5.1 Change control procedures	85
12.5.2 Technical review of applications after operating system changes.....	86
12.5.3 Restrictions on changes to software packages.....	86
12.5.4 Information leakage.....	87
12.5.5 Outsourced software development.....	87
12.6 TECHNICAL VULNERABILITY MANAGEMENT	88
12.6.1 Control of technical vulnerabilities	88
13 INFORMATION SECURITY INCIDENT MANAGEMENT	90
13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES	90
13.1.1 Reporting information security events	90
13.1.2 Reporting security weaknesses	91
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS	91
13.2.1 Responsibilities and procedures	92
13.2.2 Learning from information security incidents	93
13.2.3 Collection of evidence.....	93
14 BUSINESS CONTINUITY MANAGEMENT	95
14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	95
14.1.1 Including information security in the business continuity management process.....	95
14.1.2 Business continuity and risk assessment.....	96
14.1.3 Developing and implementing continuity plans including information security	96
14.1.4 Business continuity planning framework.....	97
14.1.5 Testing, maintaining and re-assessing business continuity plans.....	98
15 COMPLIANCE.....	100
15.1 COMPLIANCE WITH LEGAL REQUIREMENTS	100
15.1.1 Identification of applicable legislation	100
15.1.2 Intellectual property rights (IPR)	100
15.1.3 Protection of organizational records.....	101
15.1.4 Data protection and privacy of personal information	102
15.1.5 Prevention of misuse of information processing facilities	102
15.1.6 Regulation of cryptographic controls	103
15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE	103
15.2.1 Compliance with security policies and standards.....	104
15.2.2 Technical compliance checking	104
15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS	105
15.3.1 Information systems audit controls.....	105
15.3.2 Protection of information systems audit tools	105
BIBLIOGRAPHY.....	107
INDEX	108

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.