

Australian Standard™

**Information technology—Guidelines for
the management of IT Security**

Part 4: Selection of safeguards

This Australian Standard was prepared by Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 4 March 2003 and published on 29 April 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 Standards may also be withdrawn.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 Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

Australian Standard™

**Information technology—Guidelines for
the management of IT Security**

Part 4: Selection of safeguards

First published as AS 13335.4—2003.

COPYRIGHT

© Standards Australia International

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.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5111 3

PREFACE

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology. After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian, rather than an Australian New Zealand Standard.

This Standard is identical with, and has been reproduced from ISO/IEC TR 13335-4:2000, *Information technology—Guidelines for the management of IT Security, Part 4: Selection of safeguards*.

The objective of this Standard is to provide guidance on the selection of safeguards, taking into account business needs and security concerns. It describes a process for the selection of safeguards according to security risks and concerns and the specific environment of an organization.

This Standard is Part 4 of AS/NZS 13335, *Information technology—Guidelines for the management of IT Security*, which is published in parts as follows:

- Part 1: Concepts and models for IT Security
- Part 2: Managing and planning IT Security
- Part 3: Techniques for the management of IT Security
- Part 4: Selection of safeguards (this Standard)
- Part 5: Management guidance on network security

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 part of ISO/IEC TR 13335’ should read ‘this Australian Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>	<i>Australian Standard</i>
ISO/IEC	AS
TR 13335 Information technology—Guidelines for the management of IT Security	13335 Information technology—Guidelines for the management of IT Security
13335-1 Part 1: Concepts and models for IT Security	13335.1 Part 1: Concepts and models for IT Security
13335-2 Part 2: Managing and planning IT Security	13335.2 Part 2: Managing and planning IT Security
13335-3 Part 3: Techniques for the management of IT Security	13335.3 Part 3: Techniques for the management of IT Security

CONTENTS

	<i>Page</i>
1 SCOPE.....	1
2 REFERENCES	1
3 DEFINITIONS.....	1
4 AIM.....	1
5 OVERVIEW.....	2
6 INTRODUCTION TO SAFEGUARD SELECTION AND THE CONCEPT OF BASELINE SECURITY.....	4
7 BASIC ASSESSMENTS	8
7.1 IDENTIFICATION OF THE TYPE OF IT SYSTEM	8
7.2 IDENTIFICATION OF PHYSICAL/ENVIRONMENTAL CONDITIONS	8
7.3 ASSESSMENT OF EXISTING/PLANNED SAFEGUARDS	9
8 SAFEGUARDS.....	9
8.1 ORGANIZATIONAL AND PHYSICAL SAFEGUARDS	10
8.1.1 <i>IT Security Management and Policies</i>	10
8.1.2 <i>Security Compliance Checking</i>	10
8.1.3 <i>Incident Handling</i>	11
8.1.4 <i>Personnel</i>	11
8.1.5 <i>Operational Issues</i>	12
8.1.6 <i>Business Continuity Planning</i>	13
8.1.7 <i>Physical Security</i>	13
8.2 IT SYSTEM SPECIFIC SAFEGUARDS.....	18
8.2.1 <i>Identification and Authentication (I&A)</i>	18
8.2.2 <i>Logical Access Control and Audit</i>	19
8.2.3 <i>Protection against Malicious Code</i>	19
8.2.4 <i>Network Management</i>	20
8.2.5 <i>Cryptography</i>	21
9 BASELINE APPROACH: SELECTION OF SAFEGUARDS ACCORDING TO THE TYPE OF IT SYSTEM.....	24
9.1 GENERALLY APPLICABLE SAFEGUARDS	25
9.2 IT SYSTEM SPECIFIC SAFEGUARDS.....	26
10 SELECTION OF SAFEGUARDS ACCORDING TO SECURITY CONCERNS AND THREATS..	27
10.1 ASSESSMENT OF SECURITY CONCERNS	27
10.1.1 <i>Loss of confidentiality</i>	28
10.1.2 <i>Loss of integrity</i>	28
10.1.3 <i>Loss of availability</i>	28
10.1.4 <i>Loss of accountability</i>	29
10.1.5 <i>Loss of authenticity</i>	29
10.1.6 <i>Loss of reliability</i>	29
10.2 SAFEGUARDS FOR CONFIDENTIALITY	30
10.2.1 <i>Eavesdropping</i>	30

10.2.2	<i>Electromagnetic radiation</i>	30
10.2.3	<i>Malicious code</i>	31
10.2.4	<i>Masquerading of user identity</i>	31
10.2.5	<i>Misrouting/re-routing of messages</i>	31
10.2.6	<i>Software failure</i>	31
10.2.7	<i>Theft</i>	32
10.2.8	<i>Unauthorized access to computers, data, services and applications</i>	32
10.2.9	<i>Unauthorized access to storage media</i>	32
10.3	SAFEGUARDS FOR INTEGRITY	33
10.3.1	<i>Deterioration of storage media</i>	33
10.3.2	<i>Maintenance error</i>	33
10.3.3	<i>Malicious code</i>	33
10.3.4	<i>Masquerading of user identity</i>	33
10.3.5	<i>Misrouting/re-routing of messages</i>	34
10.3.6	<i>Non-Repudiation</i>	34
10.3.7	<i>Software failure</i>	34
10.3.8	<i>Supply failure (power, air conditioning)</i>	34
10.3.9	<i>Technical failure</i>	35
10.3.10	<i>Transmission errors</i>	35
10.3.11	<i>Unauthorized access to computers, data, services and applications</i>	35
10.3.12	<i>Use of unauthorized programmes and data</i>	36
10.3.13	<i>Unauthorized access to storage media</i>	36
10.3.14	<i>User error</i>	36
10.4	SAFEGUARDS FOR AVAILABILITY	36
10.4.1	<i>Destructive attack</i>	37
10.4.2	<i>Deterioration of storage media</i>	37
10.4.3	<i>Failure of communication equipment and services</i>	37
10.4.4	<i>Fire, water</i>	38
10.4.5	<i>Maintenance error</i>	38
10.4.6	<i>Malicious code</i>	38
10.4.7	<i>Masquerading of user identity</i>	38
10.4.8	<i>Misrouting/re-routing of messages</i>	39
10.4.9	<i>Misuse of resources</i>	39
10.4.10	<i>Natural disasters</i>	39
10.4.11	<i>Software failures</i>	39
10.4.12	<i>Supply failure (power, air conditioning)</i>	40
10.4.13	<i>Technical failures</i>	40
10.4.14	<i>Theft</i>	40
10.4.15	<i>Traffic overloading</i>	40
10.4.16	<i>Transmission errors</i>	41
10.4.17	<i>Unauthorized access to computers, data, services and applications</i>	41
10.4.18	<i>Use of unauthorized programmes and data</i>	41
10.4.19	<i>Unauthorized access to storage media</i>	42
10.4.20	<i>User error</i>	42
10.5	SAFEGUARDS FOR ACCOUNTABILITY, AUTHENTICITY AND RELIABILITY	42
10.5.1	<i>Accountability</i>	42
10.5.2	<i>Authenticity</i>	42
10.5.3	<i>Reliability</i>	43
11	SELECTION OF SAFEGUARDS ACCORDING TO DETAILED ASSESSMENTS	43
11.1	RELATION BETWEEN PART 3 AND PART 4 OF THIS TECHNICAL REPORT	43
11.2	PRINCIPLES OF SELECTION	43
12	DEVELOPMENT OF AN ORGANIZATION-WIDE BASELINE	45
13	SUMMARY	46
	BIBLIOGRAPHY	46

	<i>Page</i>
ANNEX A	CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT..... 47
ANNEX B	ETSI BASELINE SECURITY STANDARD FEATURES AND MECHANISMS 49
ANNEX C	IT BASELINE PROTECTION MANUAL..... 51
ANNEX D	NIST COMPUTER SECURITY HANDBOOK 53
ANNEX E	MEDICAL INFORMATICS: SECURITY CATEGORISATION AND PROTECTION FOR HEALTHCARE INFORMATION SYSTEMS 55
ANNEX F	TC68 BANKING AND RELATED FINANCIAL SERVICES - INFORMATION SECURITY GUIDELINES..... 56
ANNEX G	PROTECTION OF SENSITIVE INFORMATION NOT COVERED BY THE OFFICIAL SECRETS ACT - RECOMMENDATIONS FOR COMPUTER WORKSTATIONS..... 58
ANNEX H	CANADIAN HANDBOOK ON INFORMATION TECHNOLOGY SECURITY..... 60

AUSTRALIAN STANDARD

Information technology — Guidelines for the management of IT Security —**Part 4:
Selection of safeguards****1 Scope**

This part of ISO/IEC TR 13335 provides guidance on the selection of safeguards, taking into account business needs and security concerns. It describes a process for the selection of safeguards according to security risks and concerns and the specific environment of an organization. It shows how to achieve appropriate protection, and how this can be supported by the application of baseline security. An explanation is provided on how the approach outlined in this part of ISO/IEC TR 13335 supports the techniques for the management of IT security laid out in ISO/IEC TR 13335-3.

2 References

ISO/IEC 13335-1: 1997	Guidelines for the Management of IT Security - Part 1: Concepts and Models
ISO/IEC 13335-2: 1997	Guidelines for the Management of IT Security - Part 2: Managing and Planning IT Security
ISO/IEC 13335-3: 1997	Guidelines for the Management of IT Security - Part 3: Techniques for the Management of IT Security
ISO/IEC 10181-2: 1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework
ISO/IEC 11770-1: 1996	Key Management - Part 1: Framework

3 Terms and definitions

For the purposes of this part of ISO/IEC TR 13335, the terms defined in ISO/IEC TR 13335-1 apply: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, IT security, IT security policy, reliability, residual risk, risk, risk analysis, risk management, safeguard, system integrity, threat, and vulnerability. In addition, the following terms are used:

3.1**authentication**

provision of assurance of the claimed identity of an entity (ISO/IEC 10181-2)

3.2**identification**

process of uniquely determining the unique identity of an entity

4 Aim

The aim of this part of ISO/IEC TR 13335 is to provide guidance on the selection of safeguards. This guidance is provided for the situations where, for an IT system, a decision is taken to select