

Australian Standard™

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

**Part 5: Management guidance on
network security**

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 Standards may also be withdrawn.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 website at www.standards.com.au and looking up the relevant Standard in the online 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 5: Management guidance on
network security**

First published as AS 13335.5—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 5112 1

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 13335-5:2001, *Information technology—Guidelines for the management of IT Security, Part 5: Management guidance on network security*.

The objective of this Standard is to provide guidance to identify and analyse the communications related factors that should be taken into account when establishing network security requirements.

This Standard is Part 5 of AS 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
- Part 5: Management guidance on network security (this Standard)

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 or Australian/New Zealand 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
13335-4	Part 4: Selection of safeguards	13335.4	Part 4: Selection of safeguards
		AS/NZS	
7498	Information technology (Information processing systems)—Open Systems Interconnection—Basic reference model	2777	Information processing systems—Open Systems Interconnection—Basic reference model
7498-1	Part 1: The basic model	2777.1	Part 1: The basic model
7498-2	Part 2: Security architecture	2777.2	Part 2: Security architecture
7498-3	Part 3: Naming and addressing	2777.3	Part 3: Naming and addressing
7498-4	Part 4: Management framework	2777.4	Part 4: Management framework

CONTENTS

	<i>Page</i>
1. SCOPE	1
2. REFERENCES	1
3. DEFINITIONS	2
4. ABBREVIATIONS	2
5. STRUCTURE	2
6. AIM	3
7. OVERVIEW	3
7.1 Background	3
7.2 Identification Process	3
8 REVIEW CORPORATE IT SECURITY POLICY REQUIREMENTS	6
9 REVIEW NETWORK ARCHITECTURES AND APPLICATIONS	6
9.1 Introduction	6
9.2 Types of Network	7
9.3 Network Protocol	8
9.4 Network Applications	8
9.5 Other Considerations	8
10 IDENTIFY TYPES OF NETWORK CONNECTION	8
11 REVIEW NETWORKING CHARACTERISTICS AND RELATED TRUST RELATIONSHIPS	11
11.1 Network Characteristics	11
11.2 Trust Relationships	12

	<i>Page</i>
12 DETERMINE THE TYPES OF SECURITY RISK	13
13 IDENTIFY APPROPRIATE POTENTIAL SAFEGUARD AREAS	17
13.1 Introduction	17
13.2 Secure Service Management	18
13.2.1 Introduction	18
13.2.2 Security Operating Procedures	19
13.2.3 Security Compliance Checking	19
13.2.4 Security Conditions For Connection	19
13.2.5 Documented Security Conditions for Users of Network Services	20
13.2.6 Incident Handling	20
13.3 Identification and Authentication	20
13.3.1 Introduction	20
13.3.2 Remote Log-in	20
13.3.3 Authentication Enhancements	21
13.3.4 Remote System Identification	21
13.3.5 Secure Single Sign-on	22
13.4 Audit Trails	22
13.5 Intrusion Detection	23
13.6 Protection Against Malicious Code	24
13.7 Network Security Management	24
13.8 Security Gateways	25
13.9 Data Confidentiality Over Networks	26
13.10 Data Integrity Over Networks	26
13.11 Non-Repudiation	27
13.12 Virtual Private Networks	28
13.13 Business Continuity/Disaster Recovery	28
14 DOCUMENT AND REVIEW SECURITY ARCHITECTURE OPTIONS	29
15 PREPARE FOR THE ALLOCATION OF SAFEGUARD SELECTION, DESIGN, IMPLEMENTATION AND MAINTENANCE	29
16 SUMMARY	29
Bibliography	31

Information technology — Guidelines for the management of IT Security —

Part 5: Management guidance on network security

1. Scope

ISO/IEC TR 13335-5 provides guidance with respect to networks and communication to those responsible for the management of IT security. This guidance supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements.

This part of ISO/IEC TR 13335 builds upon Part 4 of this Technical Report by providing an introduction on how to identify appropriate safeguard areas with respect to security associated with connections to communications networks.

It is not within the scope of this TR to provide advice on the detailed design and implementation aspects of the technical safeguard areas. That advice will be dealt with in future ISO documents.

2. References

ISO/IEC TR 13335-1:1996, *Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security*

ISO/IEC TR 13335-2:1997, *Information technology — Guidelines for the management of IT Security — Part 2: Managing and planning IT Security*

ISO/IEC TR 13335-3:1998, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT Security*

ISO/IEC TR 13335-4:2000, *Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards*

ISO/IEC TR 14516:—¹⁾, *Information technology — Guidelines on the use and management of Trusted Third Party (TTP) services*

ISO/IEC 13888 (all parts), *Information technology — Security techniques — Non-repudiation*

ISO/IEC 15947:—¹⁾, *Information technology — Security techniques — IT intrusion detection framework*

ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*