AS 13335.4—2003
ISO/IEC TR 13335-4:2000

Australian Standard™

Information technology—Guidelines for the management of IT Security

Part 4: Selection of safeguards

Standards Australia

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 Standards may also be withdrawn.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.

This Standard was issued in draft form for comment as DR 02540.

Australian Standard™

Information technology—Guidelines for the management of IT Security

Part 4: Selection of safeguards

First published as AS 13335.4—2003.

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:

Reference to International Standard		*Australian Standard*	
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

Page

Page

Page

NOTES

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