AS 13335.1—2003
ISO/IEC TR 13335-1:1996

Australian Standard™

Information technology—Guidelines for the management of IT Security

Part 1: Concepts and models for IT Security

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 Standards may also be withdrawn.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 02537.

Australian Standard™

Information technology—Guidelines for the management of IT Security

Part 1: Concepts and models for IT Security

First published as AS 13335.1—2003.

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

ISBN 0 7337 5108 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 13335-1:1996, *Information technology—Guidelines for the management of IT Security,* Part 1: *Concepts and models for IT Security*.

The objective of this Standard is to provide an overview of the fundamental concepts and models used to describe the management of IT security.

This Standard is Part 1 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 (this Standard)
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

The terms 'normative' and 'informative' are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

As this Standard is reproduced from an International Technical Report, 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 '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		AS	
7498	Information processing systems—Open Systems Interconnection—Basic reference model	2777	Information processing systems—Open Systems Interconnection—Basic reference model
7498-2	Part 2: Security architecture	2777.2	Part 2: Security architecture

CONTENTS

NOTES

AUSTRALIAN STANDARD

Information technology — Guidelines for the management of IT Security —

Part 1:
Concepts and models for IT Security

1. Scope
ISO/IEC TR 13335 contains guidance on the management of IT security. Part 1 of ISO/IEC TR 13335 presents the basic management concepts and models which are essential for an introduction into the management of IT security. These concepts and models are further discussed and developed in the remaining parts to provide more detailed guidance. Together these parts can be used to help identify and manage all aspects of IT security. Part 1 is necessary for a complete understanding of the subsequent parts of ISO/IEC TR 13335.

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

3. Definitions

The following definitions are used in the three parts of ISO/IEC TR 13335.

3.1 accountability: the property that ensures that the actions of an entity may be traced uniquely to the entity (ISO 7498-2: 1989).

3.2 asset: anything that has value to the organization.

3.3 authenticity: the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.

3.4 availability: the property of being accessible and usable upon demand by an authorized entity (ISO 7498-2: 1989).

3.5 baseline controls: a minimum set of safeguards established for a system or organization.

3.6 confidentiality: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO 7498-2: 1989).

3.7 data integrity: the property that data has not been altered or destroyed in an unauthorized manner (ISO 7498-2: 1989).

3.8 impact: the result of an unwanted incident.

3.9 integrity: see data integrity and system integrity.

3.10 IT security: all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.