AS 13335.3—2003
ISO/IEC TR 13335-3:1998

Australian Standard™

Information technology—Guidelines for the management of IT Security

Part 3: Techniques for the management of 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 Standards may also be withdrawn.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 02539.

Australian Standard™

Information technology—Guidelines for the management of IT Security

Part 3: Techniques for the management of IT Security

First published as AS 13335.3—2003.

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

ISBN 0 7337 5110 5

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 13335-3:1998, *Information technology—Guidelines for the management of IT Security,* Part 3: *Techniques for the Management of IT Security.*

The objective of this Standard is to provide techniques for the management of IT security. The techniques are based on the general guidelines laid out in AS 13335.1 and AS 13335.2.

This Standard is Part 3 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 (this Standard)
Part 4: Selection of safeguards
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 13335-3' 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

CONTENTS

Page

AUSTRALIAN STANDARD

Information technology — Guidelines for the management of IT Security —

Part 3: Techniques for the management of IT Security

1 Scope

This part of ISO/IEC TR 13335 provides techniques for the management of IT security. The techniques are based on the general guidelines laid out in ISO/IEC TR 13335-1 and ISO/IEC TR 13335-2. These guidelines are designed to assist the implementation of IT security. Familiarity with the concepts and models introduced in ISO/IEC TR 13335-1 and the material concerning the management and planning of IT security in ISO/IEC TR 13335-2 is important for a complete understanding of this part of ISO/IEC TR 13335.

2 References

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

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

3 Definitions

For the purposes of this part of ISO/IEC TR 13335, the following definitions given 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.

4 Structure

This part of ISO/IEC TR 13335 is divided into 12 clauses. Clause 5 provides information on the aim of this part of ISO/IEC TR 13335. Clause 6 gives an overview of the IT security management process. Clause 7 discusses the importance of a corporate IT security policy and what it should include. Clause 8 provides an overview of four different approaches an organization may use to identify security needs. Clause 9 describes the recommended approach in detail and is followed by a description of safeguard implementation in Clause 10. This clause also includes a detailed discussion of security awareness programmes and the approval process. Clause 11 contains a description on several follow-up activities that are necessary in order to ensure that safeguards are working effectively. Finally, Clause 12 provides a brief summary of this part of ISO/IEC TR 13335.

5 Aim

The aim of this part of ISO/IEC TR 13335 is to describe and recommend techniques for the successful management of IT security. These techniques can be used to assess security requirements and risks, and help to establish and maintain the appropriate security safeguards, i.e. the correct IT security level. The results achieved in this way may need to be enhanced by additional safeguards dictated by the actual organization and environment. This part of ISO/IEC TR 13335 is relevant to everybody within an organization who is responsible for the management and/or the implementation of IT security.