AS 13335.2—2003
ISO/IEC TR 13335-2:1997

Australian Standard™

Information technology—Guidelines for the management of IT Security

Part 2: Managing and planning 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 Standards may also be withdrawn.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 02538.

Australian Standard™

Information technology—Guidelines for the management of IT Security

Part 2: Managing and planning IT Security

First published as AS 13335.2—2003.

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

ISBN 0 7337 5109 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 13335-2:1997, *Information technology—Guidelines for the management of IT Security,* Part 2: *Managing and planning IT Security*.

The objective of this Standard is to address subjects essential to the management of IT security and the relationship between those subjects, for the identification and management of all aspects of IT security.

This Standard is Part 2 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 (this Standard)
Part 3: Techniques for the management of IT Security
Part 4: Selection of safeguards
Part 5: Management of 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

CONTENTS

Page

NOTES

AUSTRALIAN STANDARD

Information technology — Guidelines for the management of IT Security —

Part 2:
Managing and planning IT Security

1 Scope

The guidelines in this part of ISO/IEC TR 13335 address subjects essential to the management of IT security, and the relationship between those subjects. These guidelines are useful for the identification and the management of all aspects of IT security.

Familiarity with the concepts and models introduced in Part 1 is essential for a complete understanding of this part.

2 Reference

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

3 Terms and definitions

For the purposes of this part of ISO/IEC TR 13335, the definitions given in ISO/IEC TR 13335-1 apply. The following terms are used: 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, vulnerability.

4 Structure

Part 2 is divided into 17 clauses. Clauses 5 and 6 provide information on the aim and background of this document. Clause 7 provides an overview of the various activities involved in successful IT security management. Clauses 8 through 16 elaborate on these activities. Clause 17 provides a summary.

5 Aim

The aim of this part is to present the different activities related to the management and the planning of IT security, as well as the associated roles and responsibilities within an organization. It is relevant to IT managers who typically have responsibility for procurement, design, implementation, or operation of IT systems. Apart from managers with responsibility for IT security, it is also relevant to managers who are responsible for activities that make substantial use of IT systems. Generally, this part is useful for anybody having managerial responsibilities relating to an organization's IT systems.

6 Background

Government and commercial organizations rely heavily on the use of information to conduct their business activities. Loss of confidentiality, integrity, availability, accountability, authenticity and reliability of information and services can have adverse impacts on organizations. Consequently, there is a critical need to protect information and to manage the security of information technology (IT) systems within organizations. This requirement to protect information is particularly important in today's environment because many organizations are internally and externally connected by networks of IT systems.

IT security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:

- determining organizational IT security objectives, strategies and policies,
- determining organizational IT security requirements,
- identifying and analyzing the security threats to, and vulnerablilities of, the assets of IT systems within the organization,
- identifying and analyzing security risks,
- specifying appropriate safeguards,
- monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization,