AS ISO/IEC 15408.3—2004
ISO/IEC 15408-3:1999

Australian Standard™

Information technology—Security techniques—Evaluation criteria for IT security

Part 3: Security assurance requirements

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 29 January 2004 and published on 17 March 2004.

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 Standards may also be withdrawn.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 Web Shop 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 Global Standard*, has a full listing of revisions and amendments published each month.

Australian Standards™ and other products and services developed by Standards Australia are published and distributed under contract by SAI Global, which operates the Standards Web Shop.

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.org.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 03551.

Australian Standard™

Information technology—Security techniques—Evaluation criteria for IT security

Part 3: Security assurance requirements

First published as AS ISO/IEC 15408.3—2004.

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

ISBN 0 7337 5768 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 15408-3:1999, *Information technology—Security techniques—Evaluation criteria for IT security*—Part 3*: Security assurance requirements*.

The objective of this Standard is to define the assurance requirements of AS ISO/IEC 15408.

This Standard is Part 3 of AS ISO/IEC 15408, *Information technology—Security techniques—Evaluation criteria for IT security*, which is published in parts as follows:

Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements (this Standard)

The term ‘informative’ has been used in this Standard to define the application of the annex to which it applies. An ‘informative’ annex is only for information and guidance.

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 15408’ should read ‘this part of AS ISO/IEC 15408’.

(c) A full point substitutes for a comma when referring to a decimal marker.

CONTENTS

Page

Page

Page

Page

List of Figures

Page

List of Tables

NOTES

AUSTRALIAN STANDARD

Information technology — Security techniques — Evaluation criteria for IT security —

Part 3:

Security assurance requirements

1 Scope

This part of ISO/IEC 15408 defines the assurance requirements of the standard. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of PPs and STs.

1.1 Organisation of ISO/IEC 15408-3

Clause 1 is the introduction and paradigm for this part of ISO/IEC 15408.

Clause 2 describes the presentation structure of the assurance classes, families, components, and evaluation assurance levels along with their relationships. It also characterises the assurance classes and families found in clauses 8 through 14.

Clauses 3, 4 and 5 provide a brief introduction to the evaluation criteria for PPs and STs, followed by detailed explanations of the families and components that are used for those evaluations.

Clause 6 provides detailed definitions of the EALs.

Clause 7 provides a brief introduction to the assurance classes and is followed by clauses 8 through 14 that provide detailed definitions of those classes.

Clauses 15 and 16 provide a brief introduction to the evaluation criteria for maintenance of assurance, followed by detailed definitions of those families and components.

Annex A provides a summary of the dependencies between the assurance components.

Annex B provides a cross reference between the EALs and the assurance components.

1.2 ISO/IEC 15408 assurance paradigm

The purpose of this subclause is to document the philosophy that underpins the ISO/IEC 15408-3 approach to assurance. An understanding of this subclause will permit the reader to understand the rationale behind the ISO/IEC 15408-3 assurance requirements.