AS ISO/IEC 15408.2—2004
ISO/IEC 15408-2:1999

Australian Standard™

Information technology—Security techniques—Evaluation criteria for IT security

Part 2: Security functional 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 Standards may also be withdrawn.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 03550.

Australian Standard™

Information technology—Security techniques—Evaluation criteria for IT security

Part 2: Security functional requirements

First published as AS ISO/IEC 15408.2—2004.

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

ISBN 0 7337 5767 7

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 15408-2:1999, *Information technology—Security techniques—Evaluation criteria for IT security*—Part 2*: Security functional requirements*.

The objective of this Standard is to define security functional components - the basis for the Target of Evaluation (TOE), the requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behavior expected of a TOE and are intended to meet the security objectives as stated in a PP or an ST; security properties that users can detect by direct interaction with the TOE (i.e., inputs, outputs) or by the TOE's response to stimulus.

This Standard is Part 2 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 (this Standard)
Part 3: Security assurance requirements

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

Page

Page

List of Figures

AUSTRALIAN STANDARD

Information technology — Security techniques — Evaluation criteria for IT security —
Part 2:
Security functional requirements

1 Scope

Security functional components, as defined in this part of ISO/IEC 15408, are the basis for the TOE IT security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction with the TOE (i.e. inputs, outputs) or by the TOE's response to stimulus.

Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organisational security policies and assumptions.

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT systems and products. ISO/IEC 15408-1 clause 3 provides additional information on the target audience of ISO/IEC 15408, and on the use of the standard by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

- Consumers who use ISO/IEC 15408-2 when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST. ISO/IEC 15408-1 subclause 4.3 provides more detailed information on the relationship between security objectives and security requirements.

- Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in this part of ISO/IEC 15408. They can also use the contents of this part of ISO/IEC 15408 as a basis for further defining the TOE security functions and mechanisms that comply with those requirements.

- Evaluators, who use the functional requirements defined in this part of ISO/IEC 15408 in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use this part of ISO/IEC 15408 to assist in determining whether a given TOE satisfies stated requirements.

1.1 Extending and maintaining functional requirements

ISO/IEC 15408 and the associated security functional requirements described herein are not meant to be a definitive answer to all the problems of IT security. Rather, the standard offers a set of well understood security functional requirements that can be used to create trusted products or systems