

Australian Standard™

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

**Part 1: Introduction and general model**

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 Standards may also be withdrawn.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](http://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](mailto:mail@standards.org.au), or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

---

Australian Standard™

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

**Part 1: Introduction and general model**

First published as AS ISO/IEC 15408.1—2004.

**COPYRIGHT**

© Standards Australia International

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

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

ISBN 0 7337 5766 9

## 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 15408-1:1999, *Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model*.

The objective of this Standard is to define criteria, which for historical and continuity purposes are referred to herein as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience. The CC will permit comparability between the results of independent security evaluations.

This Standard is Part 1 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 (this Standard)

Part 2: Security functional requirements

Part 3: Security assurance requirements

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 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 ‘ISO/IEC 15408’ should read ‘AS ISO/IEC 15408’.
- (c) A full point substitutes for a colon when referring to a decimal marker.

## CONTENTS

	<i>Page</i>
<b>1</b>	<b>Scope ..... 1</b>
<b>2</b>	<b>Definitions ..... 3</b>
2.1	Common abbreviations ..... 3
2.2	Scope of glossary ..... 3
2.3	Glossary ..... 4
<b>3</b>	<b>Overview ..... 9</b>
3.1	Introduction ..... 9
3.2	Target audience of the CC ..... 9
3.2.1	Consumers ..... 9
3.2.2	Developers ..... 10
3.2.3	Evaluators ..... 10
3.2.4	Others ..... 10
3.3	Evaluation context ..... 11
3.4	Organisation of Common Criteria ..... 12
<b>4</b>	<b>General model ..... 13</b>
4.1	Security context ..... 13
4.1.1	General security context ..... 13
4.1.2	Information technology security context ..... 15
4.2	Common Criteria approach ..... 15
4.2.1	Development ..... 16
4.2.2	TOE evaluation ..... 18
4.2.3	Operation ..... 18
4.3	Security concepts ..... 18
4.3.1	Security environment ..... 20
4.3.2	Security objectives ..... 21
4.3.3	IT security requirements ..... 22
4.3.4	TOE summary specification ..... 23
4.3.5	TC implementation ..... 23
4.4	CC descriptive material ..... 23
4.4.1	Expression of security requirements ..... 23
4.4.2	Use of security requirements ..... 25
4.4.3	Sources of security requirements ..... 27
4.5	Types of evaluation ..... 28
4.5.1	PP evaluation ..... 28
4.5.2	ST evaluation ..... 28

4.5.3	TOE evaluation .....	28
4.6	Assurance maintenance .....	28
<b>5</b>	<b>Common Criteria requirements and evaluation results .....</b>	<b>29</b>
5.1	Introduction .....	29
5.2	Requirements in PPs and STs .....	30
5.2.1	PP evaluation results .....	30
5.3	Requirements in TOE .....	30
5.3.1	TOE evaluation results .....	31
5.4	Caveats on evaluation results .....	31
5.5	Use of TOE evaluation results .....	32
<b>Annex A</b>	<b>The Common Criteria project (informative) .....</b>	<b>33</b>
A.1	Background to the Common Criteria project .....	33
A.2	Development of the Common Criteria .....	33
A.3	Common Criteria project sponsoring organisations .....	34
<b>Annex B</b>	<b>Specification of Protection Profiles .....</b>	<b>37</b>
B.1	Overview .....	37
B.2	Content of Protection Profile .....	37
B.2.1	Content and presentation .....	37
B.2.2	PP introduction .....	37
B.2.3	TOE description .....	38
B.2.4	TOE security environment .....	38
B.2.5	Security objectives .....	39
B.2.6	IT security requirements .....	40
B.2.7	Application notes .....	41
B.2.8	Rationale .....	41
<b>Annex C</b>	<b>Specification of Security Targets .....</b>	<b>43</b>
C.1	Overview .....	43
C.2	Content of Security Target .....	43
C.2.1	Content and presentation .....	43
C.2.2	ST introduction .....	43
C.2.3	TOE description .....	45
C.2.4	TOE security environment .....	45
C.2.5	Security objectives .....	46
C.2.6	IT security requirements .....	46
C.2.7	TOE summary specification .....	47
C.2.8	PP claims .....	48
C.2.9	Rationale .....	49
<b>Annex D</b>	<b>Bibliography (informative) .....</b>	<b>53</b>

**List of Figures**

Figure 3.1 - Evaluation context .....	11
Figure 4.1 - Security concepts and relationships .....	13
Figure 4.2 - Evaluation concepts and relationships .....	14
Figure 4.3 - TOE development model .....	16
Figure 4.4 - TOE evaluation process .....	17
Figure 4.5 - Derivation of requirements and specifications .....	20
Figure 4.6 - Organisation and construction of requirements .....	24
Figure 4.7 - Use of security requirements .....	26
Figure 5.1 - Evaluation results .....	29
Figure 5.2 - Use of TOE evaluation results .....	32
Figure B.1 - Protection Profile content .....	38
Figure C.1 - Security Target content .....	44

**List of Tables**

Table 3.1 - Roadmap to the Common Criteria ..... 12

Currently in preview, click buy full version

## AUSTRALIAN STANDARD

**Information technology — Security techniques — Evaluation criteria for IT security —****Part 1:****Introduction and general model****1 Scope**

This multipart standard ISO/IEC 15408 defines criteria, which for historical and continuity purposes are referred to herein as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

The CC is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. During evaluation, such an IT product or system is known as a Target of Evaluation (TOE). Such TOEs include, for example, operating systems, computer networks, distributed systems, and applications.

The CC addresses protection of information from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The CC may also be applicable to aspects of IT security outside of these three. The CC concentrates on threats to that information arising from human activities, whether malicious or otherwise, but may be applicable to some non-human threats as well. In addition, the CC may be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.

The CC is applicable to IT security measures implemented in hardware, firmware or software. Where particular aspects of evaluation are intended only to apply to certain methods of implementation, this will be indicated within the relevant criteria statements.

Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below.

- a) The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security measures. However, it is recognised that a significant part of the security of a TOE can often be achieved through administrative measures such as organisational, personnel, physical, and procedural controls. Administrative security measures in the operating environment of