

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 Standards may also be withdrawn.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.

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.

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 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

| | <i>Page</i> |
|----------|---|
| 1 | Scope 1 |
| 1.1 | Organisation of ISO/IEC 15408-3 1 |
| 1.2 | ISO/IEC 15408 assurance paradigm 1 |
| 1.2.1 | ISO/IEC 15408 philosophy 2 |
| 1.2.2 | Assurance approach 2 |
| 1.2.3 | The ISO/IEC 15408 evaluation assurance scale 4 |
| 2 | Security assurance requirements 5 |
| 2.1 | Structures 5 |
| 2.1.1 | Class structure 5 |
| 2.1.2 | Assurance family structure 6 |
| 2.1.3 | Assurance component structure 7 |
| 2.1.4 | Assurance elements 10 |
| 2.1.5 | EAL structure 10 |
| 2.1.6 | Relationship between assurances and assurance levels 13 |
| 2.2 | Component taxonomy 13 |
| 2.3 | Protection Profile and Security Target evaluation criteria class structure 13 |
| 2.4 | Usage of terms in ISO/IEC 15408-3 14 |
| 2.5 | Assurance categorisation 15 |
| 2.6 | Assurance class and family overview 15 |
| 2.6.1 | Class ACM: Configuration management 16 |
| 2.6.2 | Class ADO: Delivery and operation 17 |
| 2.6.3 | Class ADV: Development 17 |
| 2.6.4 | Class AGD: Guidance documents 18 |
| 2.6.5 | Class ALC: Lifecycle support 19 |
| 2.6.6 | Class AT: Tests 20 |
| 2.6.7 | Class AV: Vulnerability assessment 20 |
| 2.7 | Maintenance categorisation 21 |
| 2.8 | Maintenance of assurance class and family overview 21 |
| 2.8.1 | Class AMA: Maintenance of assurance 21 |
| 3 | Protection Profile and Security Target evaluation criteria 23 |
| 3.1 | Overview 23 |
| 3.2 | Protection Profile criteria overview 23 |
| 3.2.1 | Protection Profile evaluation 23 |
| 3.2.2 | Relation to the Security Target evaluation criteria 23 |
| 3.2.3 | Evaluator tasks 24 |
| 3.3 | Security Target criteria overview 24 |
| 3.3.1 | Security Target evaluation 24 |
| 3.3.2 | Relation to the other evaluation criteria in this part of ISO/IEC 15408 24 |
| 3.3.3 | Evaluator tasks 25 |
| 4 | Class APE: Protection Profile evaluation 27 |
| 4.1 | TOE description (APE_DES) 28 |
| 4.2 | Security environment (APE_ENV) 29 |
| 4.3 | PP introduction (APE_INT) 30 |

| | | |
|-----------|--|------------|
| 4.4 | Security objectives (APE_OBJ) | 31 |
| 4.5 | IT security requirements (APE_REQ) | 33 |
| 4.6 | Explicitly stated IT security requirements (APE_SRE) | 36 |
| 5 | Class ASE: Security Target evaluation | 39 |
| 5.1 | TOE description (ASE_DES) | 40 |
| 5.2 | Security environment (ASE_ENV) | 41 |
| 5.3 | ST introduction (ASE_INT) | 42 |
| 5.4 | Security objectives (ASE_OBJ) | 43 |
| 5.5 | PP claims (ASE_PPC) | 45 |
| 5.6 | IT security requirements (ASE_REQ) | 47 |
| 5.7 | Explicitly stated IT security requirements (ASE_SRE) | 49 |
| 5.8 | TOE summary specification (ASE_TSS) | 51 |
| 6 | Evaluation assurance levels | 53 |
| 6.1 | Evaluation assurance level (EAL) overview | 53 |
| 6.2 | Evaluation assurance level details | 53 |
| 6.2.1 | EAL1 - functionally tested | 55 |
| 6.2.2 | EAL2 - structurally tested | 56 |
| 6.2.3 | EAL3 - methodically tested and checked | 58 |
| 6.2.4 | EAL4 - methodically designed, tested, and reviewed | 60 |
| 6.2.5 | EAL5 - semiformally designed and tested | 62 |
| 6.2.6 | EAL6 - semiformally verified design and tested | 64 |
| 6.2.7 | EAL7 - formally verified design and tested | 66 |
| 7 | Assurance classes, families and components | 69 |
| 8 | Class ACM: Configuration management | 71 |
| 8.1 | CM automation (ACM_AUT) | 72 |
| 8.2 | CM capabilities (ACM_CAP) | 75 |
| 8.3 | CM scope (ACM_SCP) | 83 |
| 9 | Class ADO: Delivery and operation | 87 |
| 9.1 | Delivery (ADO_DEL) | 88 |
| 9.2 | Installation, generation and start-up (ADO_IGS) | 90 |
| 10 | Class ADV: Development | 93 |
| 10.1 | Functional specification (ADV_FSP) | 99 |
| 10.2 | High-level design (ADV_HLD) | 103 |
| 10.3 | Implementation representation (ADV_IMP) | 109 |
| 10.4 | TSF internals (ADV_INT) | 113 |
| 10.5 | Low-level design (ADV_LLD) | 118 |
| 10.6 | Representation correspondence (ADV_RCR) | 122 |
| 10.7 | Security policy modeling (ADV_SPM) | 125 |
| 11 | Class AGD: Guidance documents | 129 |
| 11.1 | Administrator guidance (AGD_ADM) | 130 |
| 11.2 | User guidance (AGD_USR) | 132 |

| | | |
|----------------|--|------------|
| 12 | Class ALC: Life cycle support | 135 |
| 12.1 | Development security (ALC_DVS) | 136 |
| 12.2 | Flaw remediation (ALC_FLR) | 138 |
| 12.3 | Life cycle definition (ALC_LCD) | 141 |
| 12.4 | Tools and techniques (ALC_TAT) | 145 |
| 13 | Class ATE: Tests | 149 |
| 13.1 | Coverage (ATE_COV) | 151 |
| 13.2 | Depth (ATE_DPT) | 154 |
| 13.3 | Functional tests (ATE_FUN) | 158 |
| 13.4 | Independent testing (ATE_IND) | 161 |
| 14 | Class AVA: Vulnerability assessment | 167 |
| 14.1 | Covert channel analysis (AVA_CCA) | 168 |
| 14.2 | Misuse (AVA_MSU) | 173 |
| 14.3 | Strength of TOE security functions (AVA_SOF) | 178 |
| 14.4 | Vulnerability analysis (AVA_VLA) | 180 |
| 15 | Assurance maintenance paradigm | 187 |
| 15.1 | Introduction | 187 |
| 15.2 | Assurance maintenance cycle | 188 |
| 15.2.1 | TOE acceptance | 189 |
| 15.2.2 | TOE monitoring | 191 |
| 15.2.3 | Re-evaluation | 191 |
| 15.3 | Assurance maintenance class and families | 192 |
| 15.3.1 | Assurance maintenance plan | 192 |
| 15.3.2 | TOE component categorisation report | 193 |
| 15.3.3 | Evidence of assurance maintenance | 194 |
| 15.3.4 | Security impact analysis | 195 |
| 16 | Class AMA: Maintenance of assurance | 197 |
| 16.1 | Assurance maintenance plan (AMA_AMP) | 198 |
| 16.2 | TOE component categorisation report (AMA_CAT) | 201 |
| 16.3 | Evidence of assurance maintenance (AMA_EVD) | 203 |
| 16.4 | Security impact analysis (AMA_SIA) | 205 |
| Annex A | Cross reference of assurance component dependencies | 209 |
| Annex B | Cross reference of EALs and assurance components | 213 |

List of Figures

| | |
|--|-----|
| Figure 2.1 - Assurance class/family/component/element hierarchy | 6 |
| Figure 2.2 - Assurance component structure | 8 |
| Figure 2.3 - EAL structure | 11 |
| Figure 2.4 - Assurance and assurance level association | 2 |
| Figure 2.5 - Sample class decomposition diagram | 13 |
| Figure 4.1 - Protection Profile evaluation class decomposition | 27 |
| Figure 5.1 - Security Target evaluation class decomposition | 39 |
| Figure 8.1 - Configuration management class decomposition | 71 |
| Figure 9.1 - Delivery and operation class decomposition | 87 |
| Figure 10.1 - Development class decomposition | 94 |
| Figure 10.2 - Relationships between TOE representations and requirements | 95 |
| Figure 11.1 - Guidance documents class decomposition | 129 |
| Figure 12.1 - Life-cycle support class decomposition | 135 |
| Figure 13.1 - Tests class decomposition | 150 |
| Figure 14.1 - Vulnerability assessment class decomposition | 167 |
| Figure 15.1 - Example assurance maintenance cycle | 189 |
| Figure 15.2 - Example TOE acceptance approach | 190 |
| Figure 15.3 - Example TOE monitoring approach | 191 |
| Figure 16.1 - Maintenance of assurance class decomposition | 197 |

List of Tables

| | |
|---|-----|
| Table 2.1 - Assurance family breakdown and mapping | 16 |
| Table 2.2 - Maintenance of assurance class decomposition | 21 |
| Table 3.1 - Protection Profile families - only ISO/IEC 15408 requirements | 24 |
| Table 3.2 - Protection Profile families - ISO/IEC 15408 extended requirements | 24 |
| Table 3.3 - Security Target families - only ISO/IEC 15408 requirements | 25 |
| Table 3.4 - Security Target families - ISO/IEC 15408 extended requirements | 25 |
| Table 6.1 - Evaluation assurance level summary | 54 |
| Table 6.2 - EAL1 | 55 |
| Table 6.3 - EAL2 | 57 |
| Table 6.4 - EAL3 | 59 |
| Table 6.5 - EAL4 | 61 |
| Table 6.6 - EAL5 | 63 |
| Table 6.7 - EAL6 | 65 |
| Table 6.8 - EAL7 | 67 |
| Table 15.1 - Maintenance of assurance family breakdown and mapping | 192 |
| Table A.1 - Assurance component dependencies | 209 |
| Table A.2 - AMA Internal Dependencies | 211 |
| Table B.1 - Evaluation assurance level summary | 213 |

Currently in preview, click buy full vers.

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.