INTERNATIONAL STANDARD

ISO/IEC 15408-3

First edition
1999-12-01

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

Part 3:
Security assurance requirements

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 3: Exigences d'assurance de sécurité

Reference number
ISO/IEC 15408-3:1999(E)

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

© ISO/IEC 1999

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

Contents

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: Life cycle support 19
2.6.6 Class ATE: Tests. 20
2.6.7 Class AVA: 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

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

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

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

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

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

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 12
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

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

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

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

Foreword

ISO the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, **Part 3.**

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 15408-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with Common Criteria Project Sponsoring Organisations. The identical text of ISO/IEC 15408-3 is published by the Common Criteria Project Sponsoring Organisations as *Common Criteria for Information Technology Security Evaluation.* Additional information on the Common Criteria Project and contact information on its Sponsoring Organisations is provided in Annex A of ISO-IEC 15408-1.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

- *Part 1: Introduction and general model*
- *Part 2: Security functional requirements*
- *Part 3: Security assurance requirements*

Annexes A and B of this part of ISO/IEC 15408 are for information only.

This LEGAL NOTICE has been placed in all Parts of ISO/IEC 15408 by request:
The seven governmental organisations (collectively called "the Common Criteria Project Sponsoring Organisations") identified in ISO/IEC 15408-1 Annex A, as the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluation, Parts 1 through 3 (called the "CC"), hereby grant non-exclusive license to ISO/IEC to use the CC in the development of the ISO/IEC 15408 international standard. However, the Common Criteria Project Sponsoring Organisations retain the right to use, copy, distribute, or modify the CC as they see fit.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

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.

AVA Documents Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

1.2.1 ISO/IEC 15408 philosophy

The ISO/IEC 15408 philosophy is that the threats to security and organisational security policy commitments should be clearly articulated and the proposed security measures be demonstrably sufficient for their intended purpose.

Furthermore, measures should be adopted that reduce the likelihood of vulnerabilities, the ability to exercise (i.e. intentionally exploit or unintentionally trigger) a vulnerability, and the extent of the damage that could occur from a vulnerability being exercised. Additionally, measures should be adopted that facilitate the subsequent identification of vulnerabilities and the elimination, mitigation, and/or notification that a vulnerability has been exploited or triggered.

1.2.2 Assurance approach

The ISO/IEC 15408 philosophy is to provide assurance based upon an evaluation (active investigation) of the IT product or system that is to be trusted. Evaluation has been the traditional means of providing assurance and is the basis for prior evaluation criteria documents. In aligning the existing approaches, ISO/IEC 15408 adopts the same philosophy. ISO/IEC 15408 proposes measuring the validity of the documentation and of the resulting IT product or system by expert evaluators with increasing emphasis on scope, depth, and rigour.

ISO/IEC 15408 does not exclude, nor does it comment upon, the relative merits of other means of gaining assurance. Research continues with respect to alternative ways of gaining assurance. As mature alternative approaches emerge from these research activities, they will be considered for inclusion in the standard, which is so structured as to allow their future introduction.

1.2.2.1 Significance of vulnerabilities

It is assumed that there are threat agents that will actively seek to exploit opportunities to violate security policies both for illicit gains and for well-intentioned, but nonetheless insecure actions. Threat agents may also accidentally trigger security vulnerabilities, causing harm to the organisation. Due to the need to process sensitive information and the lack of availability of sufficiently trusted products or systems, there is significant risk due to failures of IT. It is, therefore, likely that IT security breaches could lead to significant loss.

IT security breaches arise through the intentional exploitation or the unintentional triggering of vulnerabilities in the application of IT within business concerns.

Steps should be taken to prevent vulnerabilities arising in IT products and systems. To the extent feasible, vulnerabilities should be:

a) eliminated — that is, active steps should be taken to expose, and remove or neutralise, all exercisable vulnerabilities;

b) minimised — that is, active steps should be taken to reduce, to an acceptable residual level, the potential impact of any exercise of a vulnerability;

c) monitored — that is, active steps should be taken to ensure that any attempt to exercise a residual vulnerability will be detected so that steps can be taken to limit the damage.

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

1.2.2.2 Cause of vulnerabilities

Vulnerabilities can arise through failures in:

a) requirements — that is, an IT product or system may possess all the functions and features required of it and still contain vulnerabilities that render it unsuitable or ineffective with respect to security;

b) construction — that is, an IT product or system does not meet its specifications and/or vulnerabilities have been introduced as a result of poor constructional standards or incorrect design choices;

c) operation — that is, an IT product or system has been constructed correctly to a correct specification but vulnerabilities have been introduced as a result of inadequate controls upon the operation.

1.2.2.3 ISO/IEC 15408 assurance

Assurance is grounds for confidence that an IT product or system meets its security objectives. Assurance can be derived from reference to sources such as unsubstantiated assertions, prior relevant experience, or specific experience. However, the standard provides assurance through active investigation. Active investigation is an evaluation of the IT product or system in order to determine its security properties.

1.2.2.4 Assurance through evaluation

Evaluation has been the traditional means of gaining assurance, and is the basis of the ISO/IEC 15408 approach. Evaluation techniques can include, but are not limited to:

a) analysis and checking of process(es) and procedure(s);

b) checking that process(es) and procedure(s) are being applied;

c) analysis of the correspondence between TOE design representations;

d) analysis of the TOE design representation against the requirements;

e) verification of proofs;

f) analysis of guidance documents;

g) analysis of functional tests developed and the results provided;

h) independent functional testing;

i) analysis for vulnerabilities (including flaw hypothesis);

j) penetration testing.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

1.2.3 The ISO/IEC 15408 evaluation assurance scale

The ISO/IEC 15408 philosophy asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon:

a) scope — that is, the effort is greater because a larger portion of the IT product or system is included;

b) depth — that is, the effort is greater because it is deployed to a finer level of design and implementation detail;

c) rigour — that is, the effort is greater because it is applied in a more structured, formal manner.

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

2 Security assurance requirements

2.1 Structures

The following subclauses describe the constructs used in representing the assurance classes, families, components, and EALs along with the relationships among them.

Figure 2.1 illustrates the assurance requirements defined in this part of ISO/IEC 15408. Note that the most abstract collection of assurance requirements is referred to as a class. Each class contains assurance families, which then contain assurance components, which in turn contain assurance elements. Classes and families are used to provide a taxonomy for classifying assurance requirements, while components are used to specify assurance requirements in a PP/ST.

2.1.1 Class structure

Figure 2.1 illustrates the assurance class structure.

2.1.1.1 Class name

Each assurance class is assigned a unique name. The name indicates the topics covered by the assurance class.

A unique short form of the assurance class name is also provided. This is the primary means for referencing the assurance class. The convention adopted is an “A” followed by two letters related to the class name.

2.1.1.2 Class introduction

Each assurance class has an introductory subclause that describes the composition of the class and contains supportive text covering the intent of the class.

2.1.1.3 Assurance families

Each assurance class contains at least one assurance family. The structure of the assurance families is described in the following subclause.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

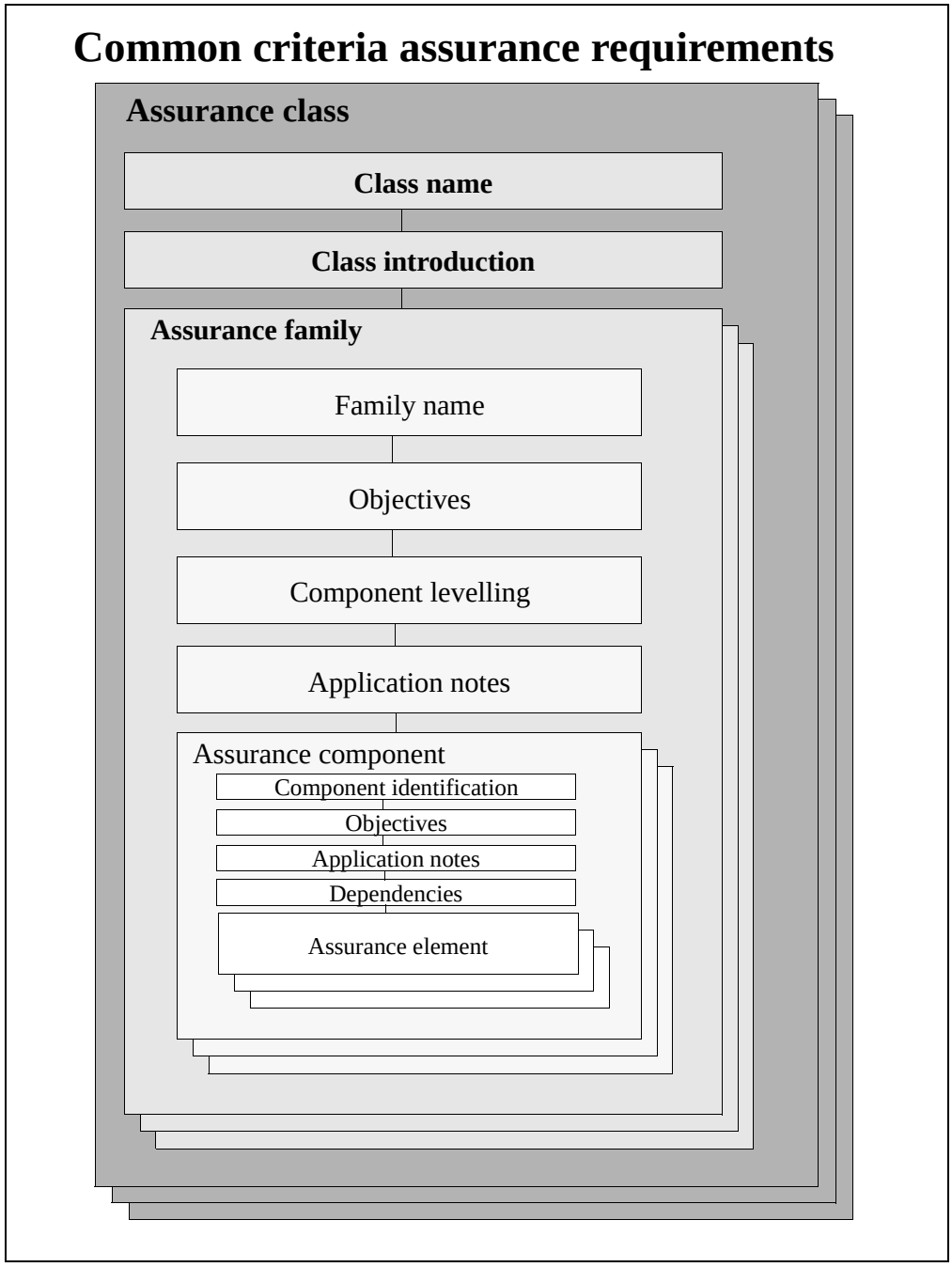

Figure 2.1 - Assurance class/family/component/element hierarchy

2.1.2 Assurance family structure

Figure 2.1 illustrates the assurance family structure.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

2.1.2.1 Family name

Every assurance family is assigned a unique name. The name provides descriptive information about the topics covered by the assurance family. Each assurance family is placed within the assurance class that contains other families with the same intent.

A unique short form of the assurance family name is also provided. This is the primary means used to reference the assurance family. The convention adopted is that the short form of the class name is used, followed by an underscore, and then three letters related to the family name.

2.1.2.2 Objectives

The objectives subclause of the assurance family presents the intent of the assurance family.

This subclause describes the objectives, particularly those related to the ISO/IEC 15408 assurance paradigm, that the family is intended to address. The description for the assurance family is kept at a general level. Any specific details required for objectives are incorporated in the particular assurance component.

2.1.2.3 Component levelling

Each assurance family contains one or more assurance components. This subclause of the assurance family describes the components available and explains the distinctions between them. Its main purpose is to differentiate between the assurance components once it has been determined that the assurance family is a necessary or useful part of the assurance requirements for a PP/ST.

Assurance families containing more than one component are levelled and rationale is provided as to how the components are levelled. This rationale is in terms of scope, depth, and/or rigour.

2.1.2.4 Application notes

The application notes subclause of the assurance family, if present, contains additional information for the assurance family. This information should be of particular interest to users of the assurance family (e.g. PP and ST authors, designers of TOEs, evaluators). The presentation is informal and covers, for example, warnings about limitations of use and areas where specific attention may be required.

2.1.2.5 Assurance components

Each assurance family has at least one assurance component. The structure of the assurance components is provided in the following subclause.

2.1.3 Assurance component structure

Figure 2.2 illustrates the assurance component structure.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

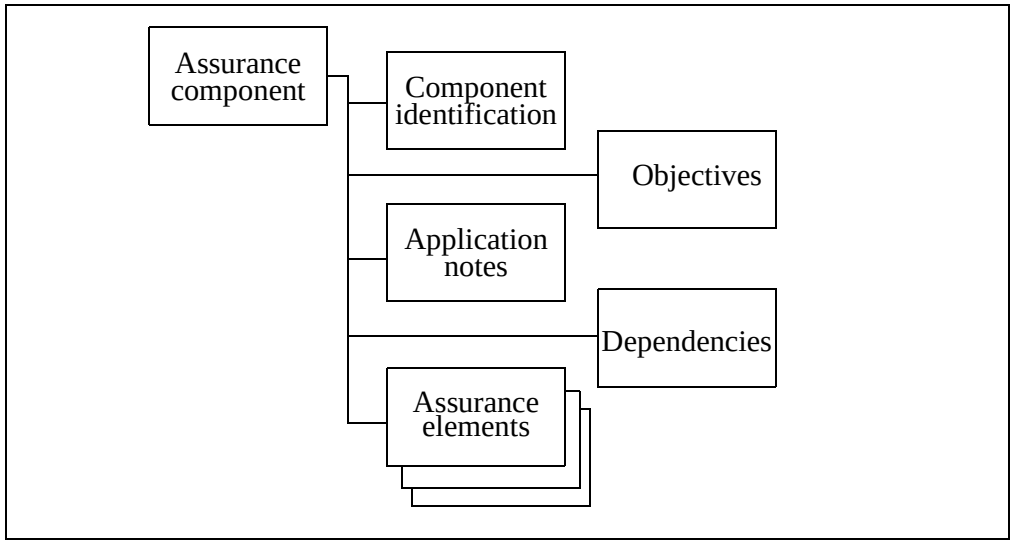

Figure 2.2 - Assurance component structure

The relationship between components within a family is highlighted using a bolding convention. Those parts of the requirements that are new, enhanced or modified beyond the requirements of the previous component within a hierarchy are bolded. The same bolding convention is also used for dependencies.

2.1.3.1 Component identification

The component identification subclause provides descriptive information necessary to identify, categorise, register, and reference a component.

Every assurance component is assigned a unique name. The name provides descriptive information about the topics covered by the assurance component. Each assurance component is placed within the assurance family that shares its security objective.

A unique short form of the assurance component name is also provided. This is the primary means used to reference the assurance component. The convention used is that the short form of the family name is used, followed by a period, and then a numeric character. The numeric characters for the components within each family are assigned sequentially, starting from 1.

2.1.3.2 Objectives

The objectives subclause of the assurance component, if present, contains specific objectives for the particular assurance component. For those assurance components that have this subclause, it presents the specific intent of the component and a more detailed explanation of the objectives.

2.1.3.3 Application notes

The application notes subclause of an assurance component, if present, contains additional information to facilitate the use of the component.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

2.1.3.4 Dependencies

Dependencies among assurance components arise when a component is not self-sufficient, and relies upon the presence of another component.

Each assurance component provides a complete list of dependencies to other assurance components. Some components may list “No dependencies”, to indicate that no dependencies have been identified. The components depended upon may have dependencies on other components.

The dependency list identifies the minimum set of assurance components which are relied upon. Components which are hierarchical to a component in the dependency list may also be used to satisfy the dependency.

In specific situations the indicated dependencies might not be applicable. The PP/ST author, by providing rationale for why a given dependency is not applicable, may elect not to satisfy that dependency.

2.1.3.5 Assurance elements

A set of assurance elements is provided for each assurance component. An assurance element is a security requirement which, if further divided, would not yield a meaningful evaluation result. It is the smallest security requirement recognised in the standard.

Each assurance element is identified as belonging to one of the three sets of assurance elements:

a) Developer action elements: the activities that shall be performed by the developer. This set of actions is further qualified by evidential material referenced in the following set of elements. Requirements for developer actions are identified by appending the letter “D” to the element number.

b) Content and presentation of evidence elements: the evidence required, what the evidence shall demonstrate, and what information the evidence shall convey. Requirements for content and presentation of evidence are identified by appending the letter “C” to the element number.

c) Evaluator action elements: the activities that shall be performed by the evaluator. This set of actions explicitly includes confirmation that the requirements prescribed in the content and presentation of evidence elements have been met. It also includes explicit actions and analysis that shall be performed in addition to that already performed by the developer. Implicit evaluator actions are also to be performed as a result of developer action elements which are not covered by content and presentation of evidence reuirements. Requirements for evaluator actions are identified by appending the letter “E” to the element number.

The developer actions and content and presentation of evidence define the assurance requirements that are used to represent a developer’s responsibilities in demonstrating assurance in the TOE security functions. By meeting these requirements, the developer can increase confidence that the TOE satisfies the functional and assurance requirements of a PP or ST.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

The evaluator actions define the evaluator's responsibilities in the two aspects of evaluation. The first aspect is validation of the PP/ST, in accordance with the classes APE and ASE in clauses 4 and 5. The second aspect is verification of the TOE's conformance with its functional and assurance requirements. By demonstrating that the PP/ST is valid and that the requirements are met by the TOE, the evaluator can provide a basis for confidence that the TOE will meet its security objectives.

The developer action elements, content and presentation of evidence elements, and explicit evaluator action elements, identify the evaluator effort that shall be expended in verifying the security claims made in the ST of the TOE.

2.1.4 Assurance elements

Each element represents a requirement to be met. These statements of requirements are intended to be clear, concise, and unambiguous. Therefore, there are no compound sentences: each separable requirement is stated as an individual element.

The elements have been written using the normal dictionary meaning for the terms used, rather than using a number of predefined terms as shorthand which results in implicit requirements. Therefore, elements are written as explicit requirements, with *no reserved terms*.

In contrast to ISO/IEC 15408-2, neither assignment nor selection operations are relevant for elements in this part of ISO/IEC 15408; however, refinements may be made to ISO/IEC 15408-3 elements as required.

2.1.5 EAL structure

Figure 2.3 illustrates the EALs and associated structure defined in this part of ISO/IEC 15408. Note that while the figure shows the contents of the assurance components, it is intended that this information would be included in an EAL by reference to the actual components defined in ISO/IEC 15408.

2.1.5.1 EAL name

Each EAL is assigned a unique name. The name provides descriptive information about the intent of the EAL.

A unique short form of the EAL name is also provided. This is the primary means used to reference the EAL.

2.1.5.2 Objectives

The objectives subclause of the EAL presents the intent of the EAL.

2.1.5.3 Application notes

The application notes subclause of the EAL, if present, contains information of particular interest to users of the EAL (e.g. PP and ST authors, designers of TOEs targeting this EAL, evaluators). The presentation is informal and covers, for example, warnings about limitations of use and areas where specific attention may be required.

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

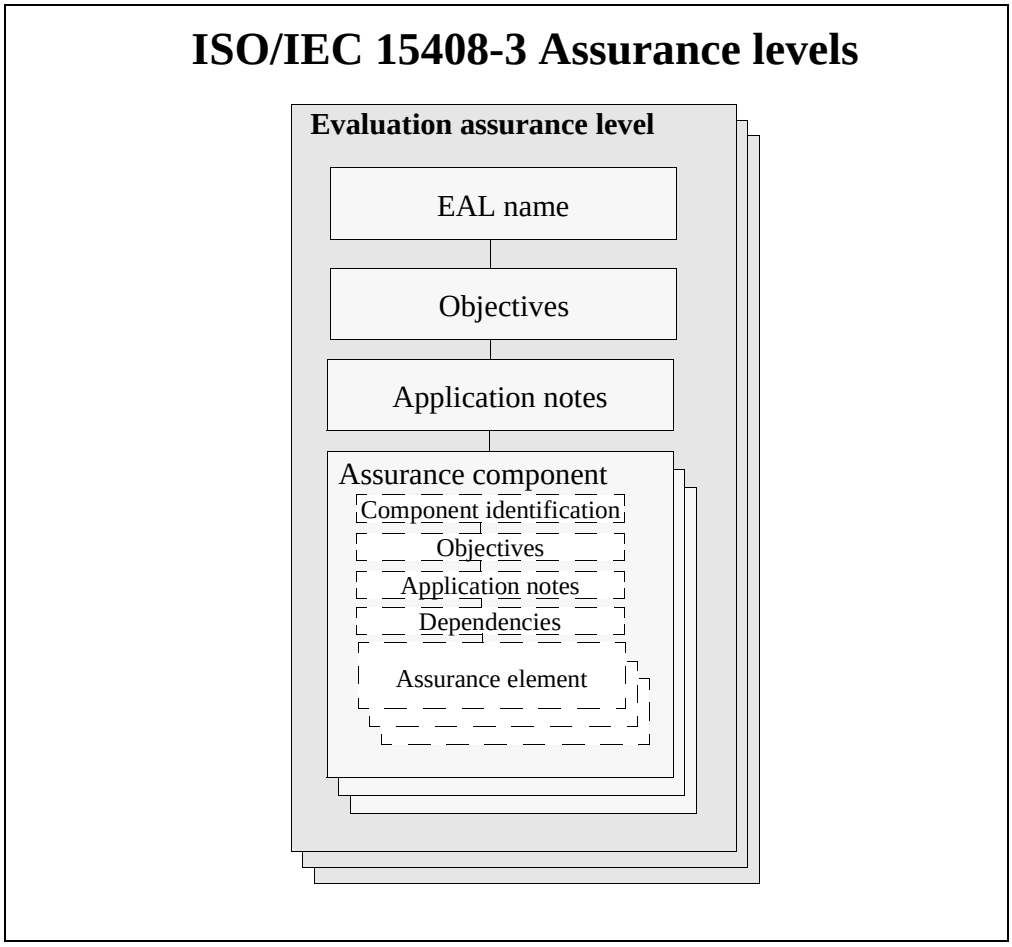

Figure 2.3 - EAL structure

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

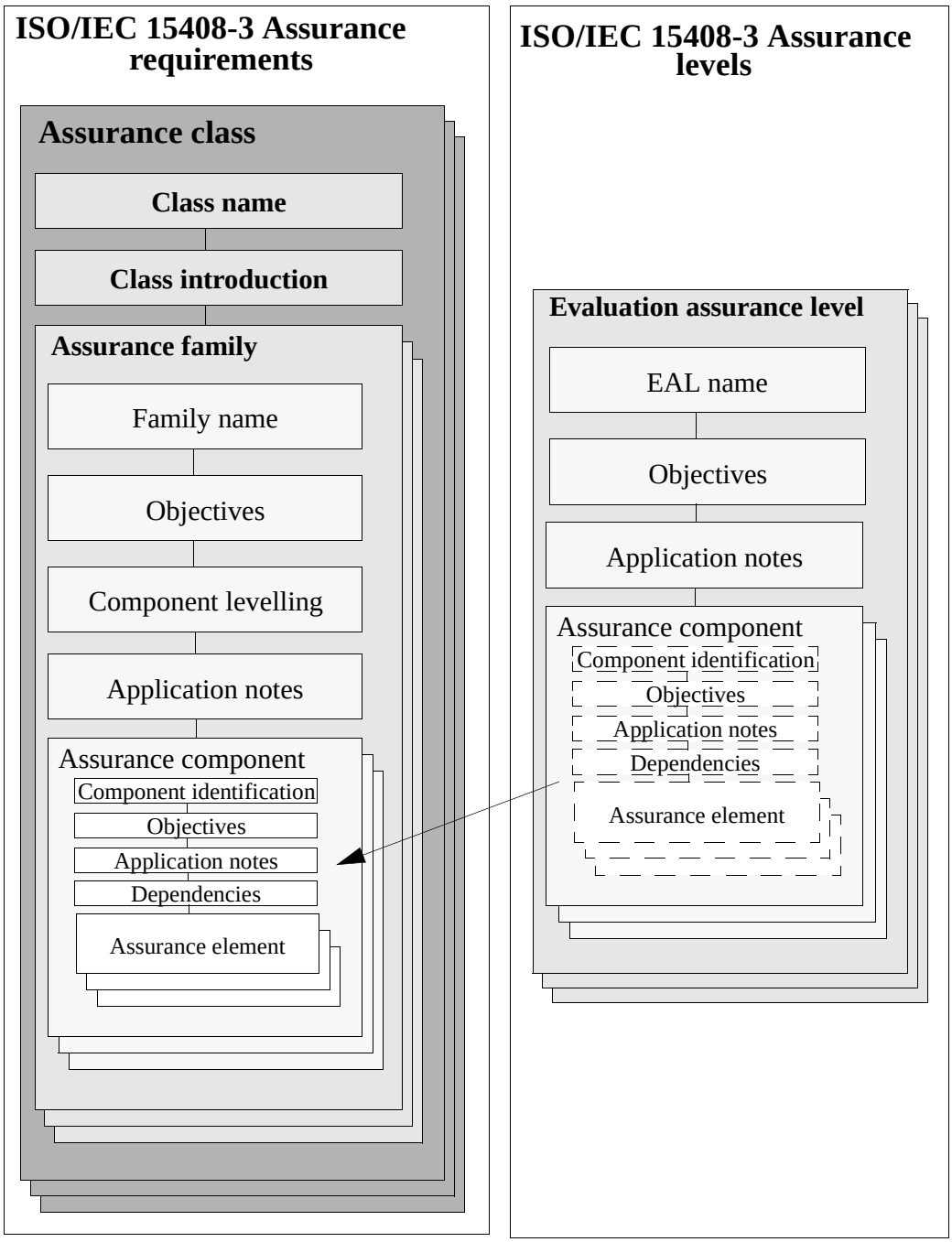

Figure 2.4 - Assurance and assurance level association

2.1.5.4 Assurance components

A set of assurance components have been chosen for each EAL.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

A higher level of assurance than that provided by a given EAL can be achieved by:

a) including additional assurance components from other assurance families; or

b) replacing an assurance component with a higher level assurance component from the same assurance family.

2.1.6 Relationship between assurances and assurance levels

Figure 2.4 illustrates the relationship between the assurance requirements and the assurance levels defined in ISO/IEC 15408. While assurance components further decompose into assurance elements, assurance elements cannot be individually referenced by assurance levels. Note that the arrow in the figure represents a reference from an EAL to an assurance component within the class where it is defined.

2.2 Component taxonomy

This part of ISO/IEC 15408 contains classes of families and components that are grouped on the basis of related assurance. At the start of each class is a diagram that indicates the families in the class and the components in each family.

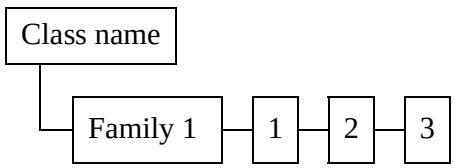

Figure 2.5 - Sample class decomposition diagram

In Figure 2.5, above, the class as shown contains a single family. The family contains three components that are linearly hierarchical (i.e. component 2 requires more than component 1, in terms of specific actions, specific evidence, or rigour of the actions or evidence). The assurance families in this part of ISO/IEC 15408 are all linearly hierarchical, although linearity is not a mandatory criterion for assurance families that may be added in the future.

2.3 Protection Profile and Security Target evaluation criteria class structure

The requirements for protection profile and security target evaluation are treated as assurance classes and are presented using the similar structure as that used for the other assurance classes, described below. One notable difference is the absence of a component levelling subclause in the associated family descriptions. The reason is that each family has only a single component and therefore no levelling has occurred.

Tables 3.1, 3.2, 3.3 and 3.4 in clause 3 of this part of ISO/IEC 15408 summarise, for both the APE and ASE classes, their constituent families and abbreviations for each. Narrative summaries for the APE families can be found in ISO/IEC 15408-1, Annex B, subclauses B.2.2 through B.2.6,

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

whereas narrative summaries for the ASE families can be found in ISO/IEC 15408-1, Annex C, subclauses C.2.2 through C.2.8.

2.4 Usage of terms in ISO/IEC 15408-3

The following is a list of terms which are used in a precise way in this part of ISO/IEC 15408. They do not merit inclusion in the glossary because they are general English terms and their usage, though restricted to the explanations given below, is in conformance with dictionary definitions. However, those explanations of the terms were used as guidance in the development of this part of ISO/IEC 15408 and should be helpful for general understanding.

Check — This term is similar to, but less rigourous than “confirm” or “verify”. This term requires a quick determination to be made by the evaluator, perhaps requiring only a cursory analysis, or perhaps no analysis at all.

Coherent — An entity is logically ordered and has a discernible meaning. For documentation, this addresses both the actual text and the structure of the document, in terms of whether it is understandable by its target audience.

Complete — All necessary parts of an entity have been provided. In terms of documentation, this means that all relevant information is covered in the documentation, at such a level of detail that no further explanation is required at that level of abstraction.

Confirm — This term is used to indicate that something needs to be reviewed in detail, and that an independent determination of sufficiency needs to be made. The level of rigour required depends on the nature of the subject matter. This term is only applied to evaluator actions.

Consistent — This term describes a relationship between two or more entities, indicating that there are no apparent contradictions between these entities.

Counter (verb) — This term is typically used in the context that a security objective counters a particular threat, but does not necessarily indicate that the threat is completely eradicated as a result.

Demonstrate — This term refers to an analysis leading to a conclusion, which is less rigourous than a “proof”.

Describe — This term requires that certain, specific details of an entity be provided.

Determine — This term requires an independent analysis to be made, with the objective of reaching a particular conclusion. The usage of this term differs from “confirm” or “verify”, since these other terms imply that an analysis has already been performed which needs to be reviewed, whereas the usage of “determine” implies a truly independent analysis, usually in the absence of any previous analysis having been performed.

Ensure — This term, used by itself, implies a strong causal relationship between an action and its consequences. This term is typically preceded by the word “helps”, which indicates that the consequence is not fully certain, on the basis of that action alone.

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

Exhaustive — This term is used in the standard with respect to conducting an analysis or other activity. It is related to "systematic" but is considerably stronger, in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to ensure that all possible avenues have been exercised.

Explain — This term differs from both "describe" and "demonstrate". It is intended to answer the question "Why?" without actually attempting to argue that the course of action that was taken was necessarily optimal.

Internally consistent — There are no apparent contradictions between any aspects of an entity. In terms of documentation, this means that there can be no statements within the documentation that can be taken to contradict each other.

Justification — This term refers to an analysis leading to a conclusion, but is more rigorous than a demonstration. This term requires significant rigour in terms of very carefully and thoroughly explaining every step of a logical argument.

Mutually supportive — This term describes a relationship between a group of entities, indicating that the entities possess properties which do not conflict with, and may assist the other entities in performing their tasks. It is not necessary to determine that every individual entity in question directly supports other entities in that grouping; rather, it is a more general determination that is made.

Prove — This refers to a formal analysis in its mathematical sense. It is completely rigourous in all ways. Typically, "prove" is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.

Specify — This term is used in the same context as "describe", but is intended to be more rigourous and precise. It is very similar to "define".

Trace (verb) — This term is used to indicate that an informal correspondence is required between two entities with only a minimal level of rigour.

Verify — This term is similar in context to "confirm", but has more rigourous connotations. This term when used in the context of evaluator actions indicates that an independent effort is required of the evaluator.

2.5 Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

2.6 Assurance class and family overview

The following summarises the assurance classes and families of clauses 8-14. These classes and family summaries are presented in the same order as they appear in clauses 8-14.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

Table 2.1 -Assurance family breakdown and mapping

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

2.6.1 Class ACM: Configuration management

Configuration management (CM) helps to ensure that the integrity of the TOE is preserved, by requiring discipline and control in the processes of refinement and modification of the TOE and other related information. CM prevents unauthorised modifications, additions, or deletions to the TOE, thus providing assurance that the TOE and documentation used for evaluation are the ones prepared for distribution.

2.6.1.1 CM automation (ACM_AUT)

Configuration management automation establishes the level of automation used to control the configuration items.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

2.6.1.2 CM capabilities (ACM_CAP)

Configuration management capabilities define the characteristics of the configuration management system.

2.6.1.3 CM scope (ACM_SCP)

Configuration management scope indicates the TOE items that need to be controlled by the configuration management system.

2.6.2 Class ADO: Delivery and operation

Assurance class ADO defines requirements for the measures, procedures, and standards concerned with secure delivery, installation, and operational use of the TOE, ensuring that the security protection offered by the TOE is not compromised during transfer, installation, start-up, and operation.

2.6.2.1 Delivery (ADO_DEL)

Delivery covers the procedures used to maintain security during transfer of the TOE to the user, both on initial delivery and as part of subsequent modification. It includes special procedures or operations required to demonstrate the authenticity of the delivered TOE. Such procedures and measures are the basis for ensuring that the security protection offered by the TOE is not compromised during transfer. While compliance with the delivery requirements cannot always be determined when a TOE is evaluated, it is possible to evaluate the procedures that a developer has developed to distribute the TOE to users.

2.6.2.2 Installation, generation and start-up (ADO_IGS)

Installation, generation, and start-up requires that the copy of the TOE is configured and activated by the administrator to exhibit the same protection properties as the master copy of the TOE. The installation, generation, and start-up procedures provide confidence that the administrator will be aware of the TOE configuration parameters and how they can affect the TSF.

2.6.3 Class ADV: Development

Assurance class ADV defines requirements for the stepwise refinement of the TSF from the TOE summary specification in the ST down to the actual implementation. Each of the resulting TSF representations provide information to help the evaluator determine whether the functional requirements of the TOE have been met.

2.6.3.1 Functional specification (ADV_FSP)

The functional specification describes the TSF, and must be a complete and accurate instantiation of the TOE security functional requirements. The functional specification also details the external interface to the TOE. Users of the TOE are expected to interact with the TSF through this interface.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

2.6.3.2 High-level design (ADV_HLD)

The high-level design is a top level design specification that refines the TSF functional specification into the major constituent parts of the TSF. The high level design identifies the basic structure of the TSF and the major hardware, firmware, and software elements.

2.6.3.3 Implementation representation (ADV_IMP)

The implementation representation is the least abstract representation of the TSF. It captures the detailed internal workings of the TSF in terms of source code, hardware drawings, etc., as applicable.

2.6.3.4 TSF internals (ADV_INT)

The TSF internals requirements specify the requisite internal structuring of the TSF.

2.6.3.5 Low-level design (ADV_LLD)

The low-level design is a detailed design specification that refines the high-level design into a level of detail that can be used as a basis for programming and/or hardware construction.

2.6.3.6 Representation correspondence (ADV_RCR)

The representation correspondence is a demonstration of mappings between all adjacent pairs of available TSF representations, from the TOE summary specification through to the least abstract TSF representation that is provided.

2.6.3.7 Security policy modeling (ADV_SPM)

Security policy models are structured representations of security policies of the TSP, and are used to provide increased assurance that the functional specification corresponds to the security policies of the TSP, and ultimately to the TOE security functional requirements. This is achieved via correspondence mappings between the functional specification, the security policy model, and the security policies that are modelled.

2.6.4 Class AGD: Guidance documents

Assurance class AGD defines requirements directed at the understandability, coverage and completeness of the operational documentation provided by the developer. This documentation, which provides two categories of information, for users and for administrators, is an important factor in the secure operation of the TOE.

2.6.4.1 Administrator guidance (AGD_ADM)

Requirements for administrative guidance help ensure that the environmental constraints can be understood by administrators and operators of the TOE. Administrative guidance is the primary means available to the developer for providing the TOE administrators with detailed, accurate information of how to administer the TOE in a secure manner and how to make effective use of the TSF privileges and protection functions.

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

2.6.4.2 User guidance (AGD_USR)

Requirements for user guidance help ensure that users are able to operate the TOE in a secure manner (e.g. the usage constraints assumed by the PP or ST must be clearly explained and illustrated). User guidance is the primary vehicle available to the developer for providing the TOE users with the necessary background and specific information on how to correctly use the TOE's protection functions. User guidance must do two things. First, it needs to explain what the user-visible security functions do and how they are to be used, so that users are able to consistently and effectively protect their information. Second, it needs to explain the user's role in maintaining the TOE's security.

2.6.5 Class ALC: Life cycle support

Assurance class ALC defines requirements for assurance through the adoption of a well defined life-cycle model for all the steps of the TOE development, including flaw remediation procedures and policies, correct use of tools and techniques and the security measures used to protect the development environment.

2.6.5.1 Development security (ALC_DVS)

Development security covers the physical, procedural, personnel, and other security measures used in the development environment. It includes physical security of the development location(s) and controls on the selection and hiring of development staff.

2.6.5.2 Flaw remediation (ALC_FLR)

Flaw remediation ensures that flaws discovered by the TOE consumers will be tracked and corrected while the TOE is supported by the developer. While future compliance with the flaw remediation requirements cannot be determined when a TOE is evaluated, it is possible to evaluate the procedures and policies that a developer has in place to track and repair flaws, and to distribute the repairs to consumers.

2.6.5.3 Life cycle definition (ALC_LCD)

Life cycle definition establishes that the engineering practices used by a developer to produce the TOE include the considerations and activities identified in the development process and operational support requirements. Confidence in the correspondence between the requirements and the TOE is greater when security analysis and the production of evidence are done on a regular basis as an integral part of the development process and operational support activities. It is not the intent of this component to dictate any specific development process.

2.6.5.4 Tools and techniques (ALC_TAT)

Tools and techniques addresses the need to define the development tools being used to analyse and implement the TOE. It includes requirements concerning the development tools and implementation dependent options of those tools.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

2.6.6 Class ATE: Tests

Assurance class ATE states testing requirements that demonstrate that the TSF satisfies the TOE security functional requirements.

2.6.6.1 Coverage (ATE_COV)

Coverage deals with the completeness of the functional tests performed by the developer on the TOE. It addresses the extent to which the TOE security functions are tested.

2.6.6.2 Depth (ATE_DPT)

Depth deals with the level of detail to which the developer tests the TOE. Testing of security functions is based upon increasing depth of information derived from analysis of the TSF representations.

2.6.6.3 Functional tests (ATE_FUN)

Functional testing establishes that the TSF exhibits the properties necessary to satisfy the requirements of its ST. Functional testing provides assurance that the TSF satisfies at least the requirements of the chosen functional components. However, functional tests do not establish that the TSF does no more than expected. This family focuses on functional testing performed by the developer.

2.6.6.4 Independent testing (ATE_IND)

Independent testing specifies the degree to which the functional testing of the TOE must be performed by a party other than the developer (e.g. a third party). This family adds value by the introduction of tests that are not part of the developers tests.

2.6.7 Class AVA: Vulnerability assessment

Assurance class AVA defines requirements directed at the identification of exploitable vulnerabilities. Specifically, it addresses those vulnerabilities introduced in the construction, operation, misuse, or incorrect configuration of the TOE.

2.6.7.1 Covert channel analysis (AVA_CCA)

Covert channel analysis is directed towards the discovery and analysis of unintended communications channels that can be exploited to violate the intended TSP.

2.6.7.2 Misuse (AVA_MSU)

Misuse analysis investigates whether an administrator or user, with an understanding of the guidance documentation, would reasonably be able to determine if the TOE is configured and operating in a manner that is insecure.

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

2.6.7.3 Strength of TOE security functions (AVA_SOF)

Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large.

2.6.7.4 Vulnerability analysis (AVA_VLA)

Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE.

2.7 Maintenance categorisation

The requirements for the maintenance of assurance are treated as an assurance class and are presented using the class structure defined above.

The maintenance of assurance families, and the abbreviation for each family are shown in Table 2.2.

Table 2.2 -Maintenance of assurance class decomposition

Assurance Class	Assurance Family	Abbreviated Name
Maintenance of assurance	Assurance maintenance plan	AMA_AMP
	TOE component categorisation report	AMA_CAT
	Evidence of assurance maintenance	AMA_EVD
	Security impact analysis	AMA_SIA

2.8 Maintenance of assurance class and family overview

The following summarises the assurance class and families of clause 16. The class and family summaries are presented in the same order as they appear in clause 16.

2.8.1 Class AMA: Maintenance of assurance

Assurance class AMA is aimed at maintaining the level of assurance that the TOE will continue to meet its security target as changes are made to the TOE or its environment. Each of the families in

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

this class identifies developer and evaluator actions that are to be applied *after* the TOE has been successfully evaluated, although some requirements can be applied at the time of the evaluation.

2.8.1.1 Assurance maintenance plan (AMA_AMP)

The assurance maintenance plan identifies the plans and procedures a developer is to implement in order to ensure that the assurance that was established in the evaluated TOE is maintained as changes are made to the TOE or its environment.

2.8.1.2 TOE component categorisation report (AMA_CAT)

The TOE component categorisation report provides a categorisation of the components of a TOE (e.g. TSF subsystems) according to their relevance to security. This categorisation acts as a focus for the developer's security impact analysis.

2.8.1.3 Evidence of assurance maintenance (AMA_EVD)

Evidence of assurance maintenance seeks to establish confidence that the assurance in the TOE is being maintained by the developer, in accordance with the assurance maintenance plan.

2.8.1.4 Security impact analysis (AMA_SIA)

Security impact analysis seeks to establish confidence that assurance has been maintained in the TOE through an analysis performed by the developer of the security impact of all changes affecting the TOE since it was evaluated.

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

3 Protection Profile and Security Target evaluation criteria

3.1 Overview

This clause introduces the evaluation criteria for PPs and STs. The evaluation criteria are then fully presented in clause 4, Class APE: Protection Profile evaluation, and clause 5, Class ASE: Security Target evaluation.

These criteria are the first requirements presented in this part of ISO/IEC 15408 because the PP and ST evaluation will normally be performed before the TOE evaluation. They play a special role in that information about the TOE is assessed and the functional and assurance requirements are evaluated in order to find out whether the PP or ST is a meaningful basis for a TOE evaluation.

Although these evaluation criteria differ somewhat from the requirements in clauses 7 through 14, they are presented in a similar manner because the developer and evaluator activities are comparable for PP, ST and TOE evaluations.

The PP and ST classes differ from the TOE classes in that all the requirements in the PP or ST class need to be considered for a PP or ST evaluation, whereas the requirements presented in the TOE classes cover a wide range of topics not all of which need be considered for a given TOE.

The evaluation criteria for PPs and STs are based on the information provided in Annexes B and C of ISO/IEC 15408-1. Useful background information for the requirements in the classes APE and ASE, as presented in the following clauses, can be found there.

3.2 Protection Profile criteria overview

3.2.1 Protection Profile evaluation

The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

3.2.2 Relation to the Security Target evaluation criteria

As described in Annexes B and C of ISO/IEC 15408-1, there are many similarities in structure and content between the generic PP and the TOE-specific ST. Consequently, the criteria for evaluating PPs contain requirements that are similar to many of those for STs, and the criteria for both are presented in a similar manner.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

3.2.3 Evaluator tasks

3.2.3.1 Evaluator tasks for an evaluation based on ISO/IEC 15408 requirements only

Evaluators performing a PP evaluation that does not include requirements from outside the standard shall apply the requirements of the APE class as described in Table 3.1.

Table 3.1 -Protection Profile families - only ISO/IEC 15408 requirements

Class	Family	Abbreviated Name
Class APE: Protection Profile evaluation	Protection Profile, TOE description	APE_DES
	Protection Profile, Security environment	APE_ENV
	Protection Profile, PP introduction	APE_INT
	Protection Profile, Security objectives	APE_OBJ
	Protection Profile, IT security requirements	APE_REQ

3.2.3.2 Evaluator tasks for a ISO/IEC 15408 extended evaluation

Evaluators performing a PP evaluation that includes requirements from outside the standard shall apply the requirements of the APE class as described in Table 3.2.

Table 3.2 -Protection Profile families - ISO/IEC 15408 extended requirements

Class	Family	Abbreviated Name
Class APE: Protection Profile evaluation	Protection Profile, TOE description	APE_DES
	Protection Profile, Security environment	APE_ENV
	Protection Profile, PP introduction	APE_INT
	Protection Profile, Security objectives	APE_OBJ
	Protection Profile, IT security requirements	APE_REQ
	Protection Profile, Explicitly stated IT security requirements	**APE_SRE**

3.3 Security Target criteria overview

3.3.1 Security Target evaluation

The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

3.3.2 Relation to the other evaluation criteria in this part of ISO/IEC 15408

There are two identified stages for the evaluation of a TOE; the ST evaluation and the corresponding TOE evaluation. The requirements for ST evaluations are discussed here and in clause 6 while the requirements for TOE evaluations are contained in clauses 7 through 14.

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

An ST evaluation includes a PP claims evaluation. If the ST does not claim PP conformance, the PP claims part of the ST shall contain a statement that the TOE does not claim conformance to any PP.

3.3.3 Evaluator tasks

3.3.3.1 Evaluator tasks for an evaluation based on ISO/IEC 15408 requirements only

Evaluators performing an ST evaluation that does not include requirements from outside the standard shall apply the requirements of the ASE class as described in Table 3.3.

Table 3.3 -Security Target families - only ISO/IEC 15408 requirements

Class	Family	Abbreviated Name
Class ASE: Security Target evaluation	Security Target, TOE description	ASE_DES
	Security Target, Security environment	ASE_ENV
	Security Target, ST introduction	ASE_INT
	Security Target, Security objectives	ASE_OBJ
	Security Target, PP claims	ASE_PPC
	Security Target, IT security requirements	ASE_REQ
	Security Target, TOE summary specification	ASE_TSS

3.3.3.2 Evaluator tasks for a ISO/IEC 15408 extended evaluation

Evaluators performing an ST evaluation that includes requirements from outside the standard shall apply the requirements of the ASE class as described in Table 3.4.

Table 3.4 -Security Target families - ISO/IEC 15408 extended requirements

Class	Family	Abbreviated Name
Class ASE: Security Target evaluation	Security Target, TOE description	ASE_DES
	Security Target, Security environment	ASE_ENV
	Security Target, ST introduction	ASE_INT
	Security Target, Security objectives	ASE_OBJ
	Security Target, PP claims	ASE_PPC
	Security Target, IT security requirements	ASE_REQ
	Security Target, Explicitly stated IT security requirements	**ASE_SRE**
	Security Target, TOE summary specification	ASE_TSS

Documents Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

4 Class APE: Protection Profile evaluation

The goal of a PP evaluation is to demonstrate that the PP is complete, consistent and technically sound. An evaluated PP is suitable for use as the basis for the development of STs. Such a PP is eligible for inclusion in a registry.

Figure 4.1 shows the families within this class.

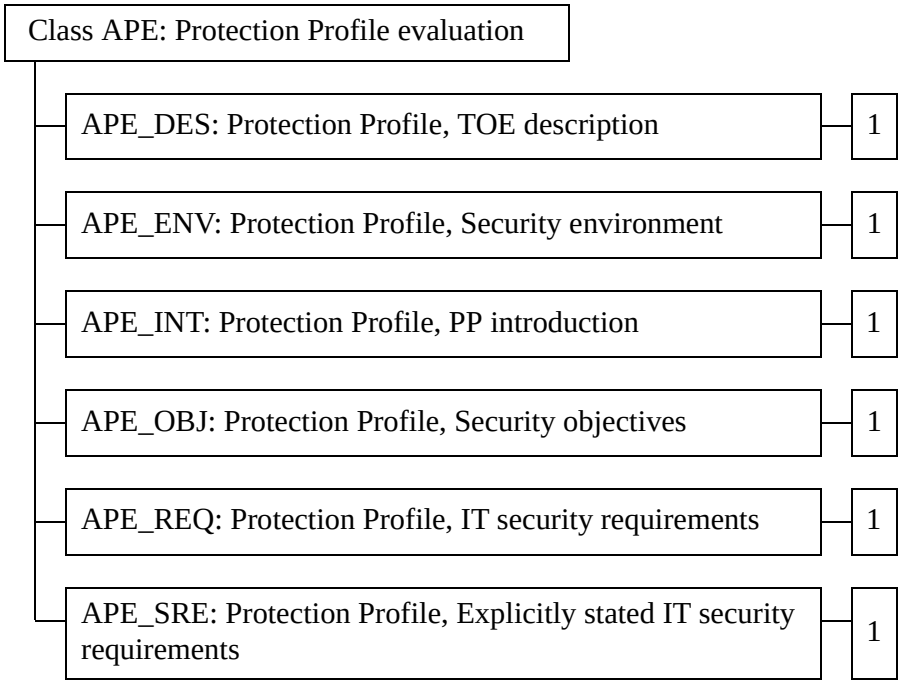

Figure 4.1 - Protection Profile evaluation class decomposition

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

4.1 TOE description (APE_DES)

Objectives

The TOE description is an aid to the understanding of the TOE's security requirements. Evaluation of the TOE description is required to show that it is coherent, internally consistent and consistent with all other parts of the PP.

APE_DES.1 Protection Profile, TOE description, Evaluation requirements

Dependencies:

APE_ENV.1 Protection Profile, Security environment, Evaluation requirements

APE_INT.1 Protection Profile, PP introduction, Evaluation requirements

APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

APE_REQ.1 Protection Profile, IT security requirements, Evaluation requirements

Developer action elements:

APE_DES.1.1D **The PP developer shall provide a TOE description as part of the PP.**

Content and presentation of evidence elements:

APE_DES.1.1C **The TOE description shall as a minimum describe the product type and the general IT features of the TOE.**

Evaluator action elements:

APE_DES.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

APE_DES.1.2E **The evaluator shall confirm that the TOE description is coherent and internally consistent.**

APE_DES.1.3E **The evaluator shall confirm that the TOE description is consistent with the other parts of the PP.**

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

4.2 Security environment (APE_ENV)

Objectives

In order to determine whether the IT security requirements in the PP are sufficient, it is important that the security problem to be solved is clearly understood by all parties to the evaluation.

APE_ENV.1 Protection Profile, Security environment, Evaluation requirements

Dependencies:

No dependencies.

Developer action elements:

APE_ENV.1.1D **The PP developer shall provide a statement of TOE security environment as part of the PP.**

Content and presentation of evidence elements:

APE_ENV.1.1C **The statement of TOE security environment shall identify and explain any assumptions about the intended usage of the TOE and the environment of use of the TOE.**

APE_ENV.1.2C **The statement of TOE security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment.**

APE_ENV.1.3C **The statement of TOE security environment shall identify and explain any organisational security policies with which the TOE must comply.**

Evaluator action elements:

APE_ENV.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

APE_ENV.1.2E **The evaluator shall confirm that the statement of TOE security environment is coherent and internally consistent.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

4.3 PP introduction (APE_INT)

Objectives

The PP introduction contains document management and overview information necessary to operate a PP registry. Evaluation of the PP introduction is required to demonstrate that the PP is correctly identified and that it is consistent with all other parts of the PP.

APE_INT.1 Protection Profile, PP introduction, Evaluation requirements

Dependencies:

APE_DES.1 Protection Profile, TOE description, Evaluation requirements

APE_ENV.1 Protection Profile, Security environment, Evaluation requirements

APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

APE_REQ.1 Protection Profile, IT security requirements, Evaluation requirements

Developer action elements:

APE_INT.1.1D **The PP developer shall provide a PP introduction as part of the PP.**

Content and presentation of evidence elements:

APE_INT.1.1C **The PP introduction shall contain a PP identification that provides the labelling and descriptive information necessary to identify, catalogue, register, and cross reference the PP.**

APE_INT.1.2C **The PP introduction shall contain a PP overview which summarises the PP in narrative form.**

Evaluator action elements:

APE_INT.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

APE_INT.1.2E **The evaluator shall confirm that the PP introduction is coherent and internally consistent.**

APE_INT.1.3E **The evaluator shall confirm that the PP introduction is consistent with the other parts of the PP.**

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

4.4 Security objectives (APE_OBJ)

Objectives

The security objectives is a concise statement of the intended response to the security problem. Evaluation of the security objectives is required to demonstrate that the stated objectives adequately address the security problem. The security objectives are categorised as security objectives for the TOE and as security objectives for the environment. The security objectives for both the TOE and the environment must be shown to be traced back to the identified threats to be countered and/or policies and assumptions to be met by each.

APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

Dependencies:

APE_ENV.1 Protection Profile, Security environment, Evaluation requirements

Developer action elements:

APE_OBJ.1.1D **The PP developer shall provide a statement of security objectives as part of the PP.**

APE_OBJ.1.2D **The PP developer shall provide the security objectives rationale.**

Content and presentation of evidence elements:

APE_OBJ.1.1C **The statement of security objectives shall define the security objectives for the TOE and its environment.**

APE_OBJ.1.2C **The security objectives for the TOE shall be clearly stated and traced back to aspects of the identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE.**

APE_OBJ.1.3C **The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats not completely countered by the TOE and/ or organisational security policies or assumptions not completely met by the TOE.**

APE_OBJ.1.4C **The security objectives rationale shall demonstrate that the stated security objectives are suitable to counter the identified threats to security.**

APE_OBJ.1.5C **The security objectives rationale shall demonstrate that the stated security objectives are suitable to cover all of the identified organisational security policies and assumptions.**

Evaluator action elements:

APE_OBJ.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

APE_OBJ.1.2E **The evaluator shall confirm that the statement of security objectives is complete, coherent, and internally consistent.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

4.5 IT security requirements (APE_REQ)

Objectives

The IT security requirements chosen for a TOE and presented or cited in a PP need to be evaluated in order to confirm that they are internally consistent and lead to the development of a TOE that will meet its security objectives.

Not all of the security objectives expressed in a PP may be met by a compliant TOE, as some TOEs may depend on certain IT security requirements to be met by the IT environment. When this is the case, the environmental IT security requirements must be clearly stated and evaluated in context with the TOE requirements.

This family presents evaluation requirements that permit the evaluator to determine that a PP is suitable for use as a statement of requirements for an evaluatable TOE. The additional criteria necessary for the evaluation of explicitly stated requirements is covered in the APE_SRE family.

Application notes

The term “IT security requirements” refers to “TOE security requirements” and the optionally included “security requirements for the IT environment”.

The term “TOE security requirements” refers to “TOE security functional requirements” and/or “TOE security assurance requirements”.

In the APE_REQ.1 component, the word “appropriate” is used to indicate that certain elements allow options in certain cases. Which options are applicable depends on the given context in the PP. Detailed information for all these aspects is contained in ISO/IEC 15408-1, Annex B.

APE_REQ.1 Protection Profile, IT security requirements, Evaluation requirements

Dependencies:

APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

Developer action elements:

APE_REQ.1.1D **The PP developer shall provide a statement of IT security requirements as part of the PP.**

APE_REQ.1.2D **The PP developer shall provide the security requirements rationale.**

Content and presentation of evidence elements:

APE_REQ.1.1C **The statement of TOE security functional requirements shall identify the TOE security functional requirements drawn from ISO/IEC 15408-2 functional requirements components.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

APE_REQ.1.2C **The statement of TOE security assurance requirements shall identify the TOE security assurance requirements drawn from ISO/IEC 15408-3 assurance requirements components.**

APE_REQ.1.3C **The statement of TOE security assurance requirements should include an Evaluation Assurance Level (EAL) as defined in ISO/IEC 15408-3.**

APE_REQ.1.4C **The evidence shall justify that the statement of TOE security assurance requirements is appropriate.**

APE_REQ.1.5C **The PP shall, if appropriate, identify any security requirements for the IT environment.**

APE_REQ.1.6C **All completed operations on IT security requirements included in the PP shall be identified.**

APE_REQ.1.7C **Any uncompleted operations on IT security requirements included in the PP shall be identified.**

APE_REQ.1.8C **Dependencies among the IT security requirements included in the PP should be satisfied.**

APE_REQ.1.9C **The evidence shall justify why any non-satisfaction of dependencies is appropriate.**

APE_REQ.1.10C **The PP shall include a statement of the minimum strength of function level for the TOE security functional requirements, either SOF-basic, SOF-medium or SOF-high, as appropriate.**

APE_REQ.1.11C **The PP shall identify any specific TOE security functional requirements for which an explicit strength of function is appropriate, together with the specific metric.**

APE_REQ.1.12C **The security requirements rationale shall demonstrate that the minimum strength of function level for the PP, together with any explicit strength of function claim, is consistent with the security objectives for the TOE.**

APE_REQ.1.13C **The security requirements rationale shall demonstrate that the IT security requirements are suitable to meet the security objectives.**

APE_REQ.1.14C **The security requirements rationale shall demonstrate that the set of IT security requirements together forms a mutually supportive and internally consistent whole.**

Evaluator action elements:

APE_REQ.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

APE_REQ.1.2E **The evaluator shall confirm that the statement of IT security requirements is complete, coherent, and internally consistent.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

4.6 Explicitly stated IT security requirements (APE_SRE)

Objectives

If, after careful consideration, none of the requirements components in ISO/IEC 15408-2 or ISO/IEC 15408-3 are readily applicable to all or parts of the IT security requirements, the PP author may state other requirements which do not reference ISO/IEC 15408. The use of such requirements shall be justified.

This family presents evaluation requirements that permit the evaluator to determine that the explicitly stated requirements are clearly and unambiguously expressed. The evaluation of requirements taken from ISO/IEC 15408 in conjunction with valid explicitly stated security requirements is addressed by the APE_REQ family.

Explicitly stated IT security requirements for a TOE presented or cited in a PP need to be evaluated in order to demonstrate that they are clearly and unambiguously expressed.

Application notes

Formulation of the explicitly stated requirements in a structure comparable to those of existing ISO/IEC 15408 components and elements involves choosing similar labelling, manner of expression, and level of detail.

Using the ISO/IEC 15408 requirements as a model means that the requirements can be clearly identified, that they are self-contained, and that the application of each requirement is feasible and will yield a meaningful evaluation result based on a compliance statement of the TOE for that particular requirement.

The term “IT security requirements” refers to “TOE security requirements” and the optionally included “security requirements for the IT environment”.

The term “TOE security requirements” refers to “TOE security functional requirements” and/or “TOE security assurance requirements”.

APE_SRE.1 Protection Profile, Explicitly stated IT security requirements, Evaluation requirements

Dependencies:

APE_REQ.1 Protection Profile, IT security requirements, Evaluation requirements

Developer action elements:

APE_SRE.1.1D **The PP developer shall provide a statement of IT security requirements as part of the PP.**

APE_SRE.1.2D **The PP developer shall provide the security requirements rationale.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

Content and presentation of evidence elements:

APE_SRE.1.1C **All TOE security requirements that are explicitly stated without reference to ISO/IEC 15408 shall be identified.**

APE_SRE.1.2C **All security requirements for the IT environment that are explicitly stated without reference to ISO/IEC 15408 shall be identified.**

APE_SRE.1.3C **The evidence shall justify why the security requirements had to be explicitly stated.**

APE_SRE.1.4C **The explicitly stated IT security requirements shall use the ISO/IEC 15408 requirements components, families and classes as a model for presentation.**

APE_SRE.1.5C **The explicitly stated IT security requirements shall be measurable and state objective evaluation requirements such that compliance or noncompliance of a TOE can be determined and systematically demonstrated.**

APE_SRE.1.6C **The explicitly stated IT security requirements shall be clearly and unambiguously expressed.**

APE_SRE.1.7C **The security requirements rationale shall demonstrate that the assurance requirements are applicable and appropriate to support any explicitly stated TOE security functional requirements.**

Evaluator action elements:

APE_SRE.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

APE_SRE.1.2E **The evaluator shall determine that all of the dependencies of the explicitly stated IT security requirements have been identified.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

Documents
Document Sharing Hub

Full document details: ISO_IEC 15408-3_1999

5 Class ASE: Security Target evaluation

The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Figure 5.1 shows the families within this class.

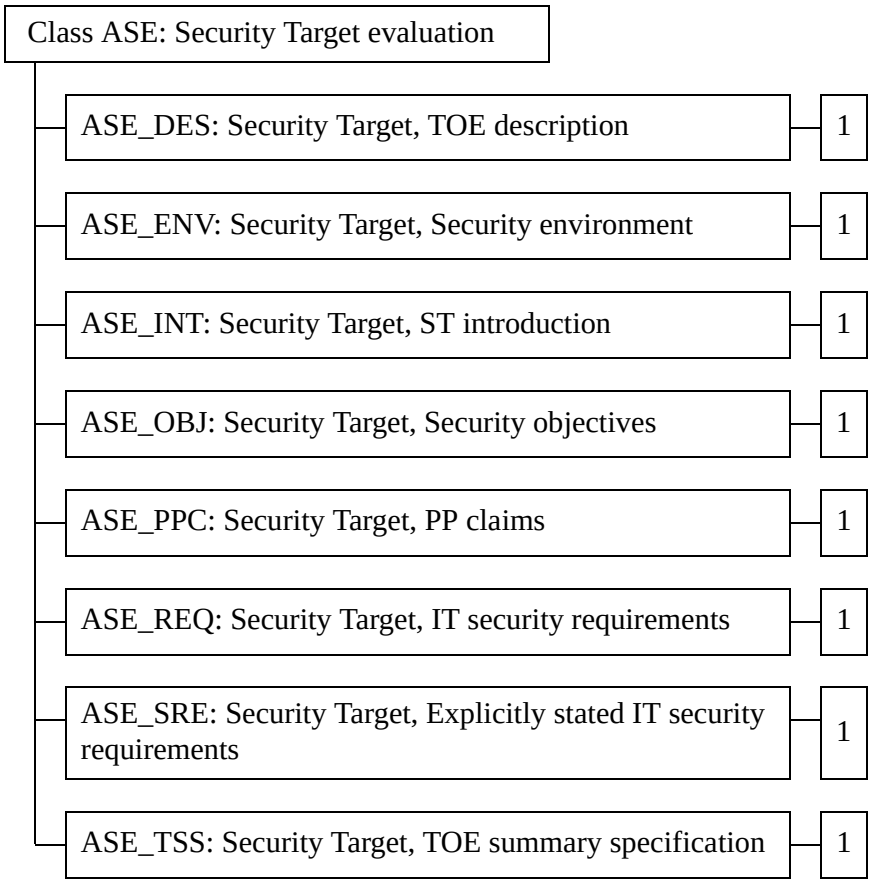

Figure 5.1 - Security Target evaluation class decomposition

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

5.1 TOE description (ASE_DES)

Objectives

The TOE description is an aid to the understanding of the TOE's security requirements. Evaluation of the TOE description is required to show that it is coherent, internally consistent and consistent with all other parts of the ST.

ASE_DES.1 Security Target, TOE description, Evaluation requirements

Dependencies:

ASE_ENV.1 Security Target, Security environment, Evaluation requirements

ASE_INT.1 Security Target, ST introduction, Evaluation requirements

ASE_OBJ.1 Security Target, Security objectives, Evaluation requirements

ASE_PPC.1 Security Target, PP claims, Evaluation requirements

ASE_REQ.1 Security Target, IT security requirements, Evaluation requirements

ASE_TSS.1 Security Target, TOE summary specification, Evaluation requirements

Developer action elements:

ASE_DES.1.1D **The developer shall provide a TOE description as part of the ST.**

Content and presentation of evidence elements:

ASE_DES.1.1C **The TOE description shall as a minimum describe the product or system type, and the scope and boundaries of the TOE in general terms both in a physical and a logical way.**

Evaluator action elements:

ASE_DES.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

ASE_DES.1.2E **The evaluator shall confirm that the TOE description is coherent and internally consistent.**

ASE_DES.1.3E **The evaluator shall confirm that the TOE description is consistent with the other parts of the ST.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

5.2 Security environment (ASE_ENV)

Objectives

In order to determine whether the IT security requirements in the ST are sufficient, it is important that the security problem to be solved is clearly understood by all parties to the evaluation.

ASE_ENV.1 Security Target, Security environment, Evaluation requirements

Dependencies:

No dependencies.

Developer action elements:

ASE_ENV.1.1D **The developer shall provide a statement of TOE security environment as part of the ST.**

Content and presentation of evidence elements:

ASE_ENV.1.1C **The statement of TOE security environment shall identify and explain any assumptions about the intended usage of the TOE and the environment of use of the TOE.**

ASE_ENV.1.2C **The statement of TOE security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment.**

ASE_ENV.1.3C **The statement of TOE security environment shall identify and explain any organisational security policies with which the TOE must comply.**

Evaluator action elements:

ASE_ENV.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

ASE_ENV.1.2E **The evaluator shall confirm that the statement of TOE security environment is coherent and internally consistent.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999

5.3 ST introduction (ASE_INT)

Objectives

The ST introduction contains identification and indexing material. Evaluation of the ST introduction is required to demonstrate that the ST is correctly identified and that it is consistent with all other parts of the ST.

ASE_INT.1 Security Target, ST introduction, Evaluation requirements

Dependencies:

ASE_DES.1 Security Target, TOE description, Evaluation requirements

ASE_ENV.1 Security Target, Security environment, Evaluation requirements

ASE_OBJ.1 Security Target, Security objectives, Evaluation requirements

ASE_PPC.1 Security Target, PP claims, Evaluation requirements

ASE_REQ.1 Security Target, IT security requirements, Evaluation requirements

ASE_TSS.1 Security Target, TOE summary specification, Evaluation requirements

Developer action elements:

ASE_INT.1.1D **The developer shall provide an ST introduction as part of the ST.**

Content and presentation of evidence elements:

ASE_INT.1.1C **The ST introduction shall contain an ST identification that provides the labelling and descriptive information necessary to control and identify the ST and the TOE to which it refers.**

ASE_INT.1.2C **The ST introduction shall contain an ST overview which summarises the ST in narrative form.**

ASE_INT.1.3C **The ST introduction shall contain a ISO/IEC 15408 conformance claim that states any evaluatable claim of ISO/IEC 15408 conformance for the TOE.**

Evaluator action elements:

ASE_INT.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

ASE_INT.1.2E **The evaluator shall confirm that the ST introduction is coherent and internally consistent.**

ASE_INT.1.3E **The evaluator shall confirm that the ST introduction is consistent with the other parts of the ST.**

Documents
Document Sharing Hub
Full document details: ISO_IEC 15408-3_1999