INTERNATIONAL STANDARD

ISO/IEC 15408-3

Second edition
2005-10-01

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

Reference number
ISO/IEC 15408-3:2005(E)

© ISO/IEC 2005

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005

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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

 © ISO/IEC 2005 – All rights reserved

Contents

Page

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15408-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information Technology Security Evaluation.

This second edition cancels and replaces the first edition (ISO/IEC 15408-3:1999), which has been technically revised.

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*

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations, version 2.3 Parts 1 through 3 (called CC 2.3), they hereby grant non-exclusive license to ISO/IEC to use CC 2.3 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC 2.3 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;

© ISO/IEC 2005 - All rights reserved

France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

Introduction

Security assurance components, as defined in this part of ISO/IEC 15408, are the basis for the security assurance requirements expressed in a Protection Profile (PP) or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This part of ISO/IEC 15408 catalogues the set of assurance components, families and classes. This part of ISO/IEC 15408 also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT systems and products. ISO/IEC 15408-1 Clause 5 provides additional information on the target audience of ISO/IEC 15408, and on the use of ISO/IEC 15408 by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

a) Consumers, who use this part of ISO/IEC 15408 when selecting components to express assurance requirements to satisfy the security objectives expressed in a PP or ST, determining required levels of security assurance of the TOE. ISO/IEC 15408-1 Subclause 5.3 provides more detailed information on the relationship between security objectives and security requirements.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this part of ISO/IEC 15408 when interpreting statements of assurance requirements and determining assurance approaches of TOEs.

c) Evaluators, who use the assurance requirements defined in this part of ISO/IEC 15408 as mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

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 ISO/IEC 15408. 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.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 15408-1 apply.

4 Overview

4.1 Organisation of this part of ISO/IEC 15408

Clause 5 describes the paradigm used in the security assurance requirements of this part of ISO/IEC 15408.

Clause 6 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 12 through 18.

Clauses 7, 8 and 9 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 10 provides detailed definitions of the EALs.

Clause 11 provides a brief introduction to the assurance classes and is followed by clauses 12 through 18 that provide detailed definitions of those classes.

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

5 ISO/IEC 15408 assurance paradigm

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

5.1 ISO/IEC 15408 philosophy

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.

5.2 Assurance approach

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 ISO/IEC 15408, which is so structured as to allow their future introduction.

5.2.1 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

5.2.2 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.

5.2.3 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, ISO/IEC 15408 provides assurance through active investigation. Active investigation is an evaluation of the IT product or system in order to determine its security properties.

5.2.4 Assurance through evaluation

Evaluation has been the traditional means of gaining assurance, and is the basis of 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.

5.3 ISO/IEC 15408 evaluation assurance scale

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

6 Security assurance requirements

6.1 Structures

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

Figure 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.

6.1.1 Class structure

Figure 1 illustrates the assurance class structure.

6.1.1.1 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.

6.1.1.2 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.

6.1.1.3 Assurance families

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

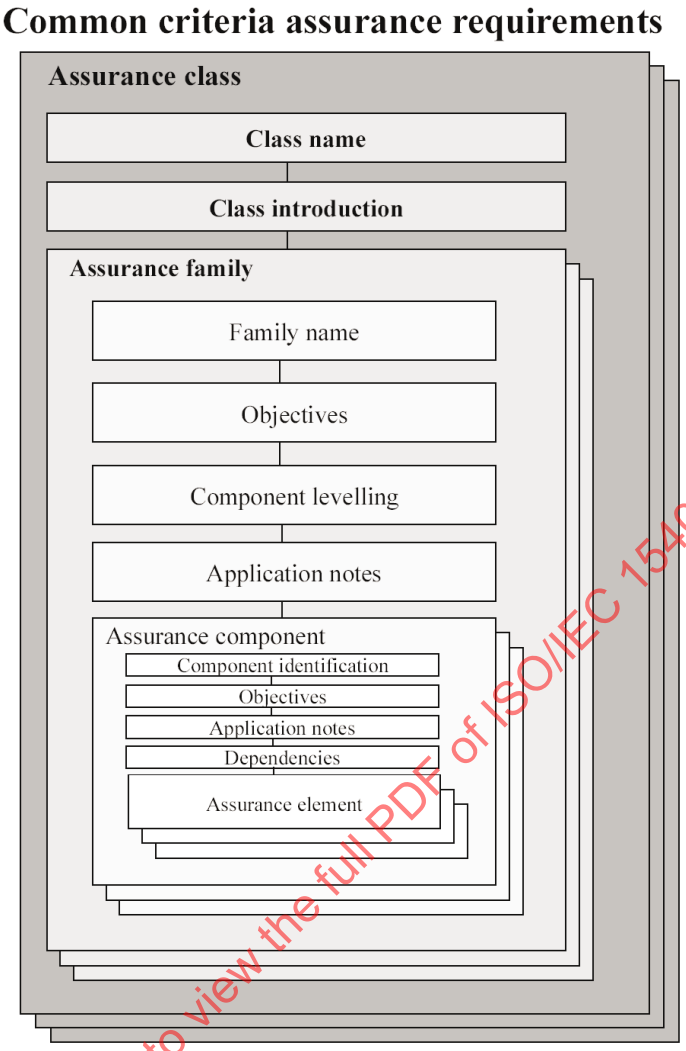


Figure 1 - Assurance class/family/component/element hierarchy

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

6.1.2 Assurance family structure

Figure 1 illustrates the assurance family structure.

6.1.2.1 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.

6.1.2.2 Objectives

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

This subclause describes the objectives, particularly those related to 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.

© ISO/IEC 2005 - All rights reserved

6.1.2.3 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.

6.1.2.4 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.

6.1.2.5 Assurance components

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

6.1.3 Assurance component structure

Figure 2 illustrates the assurance component structure.

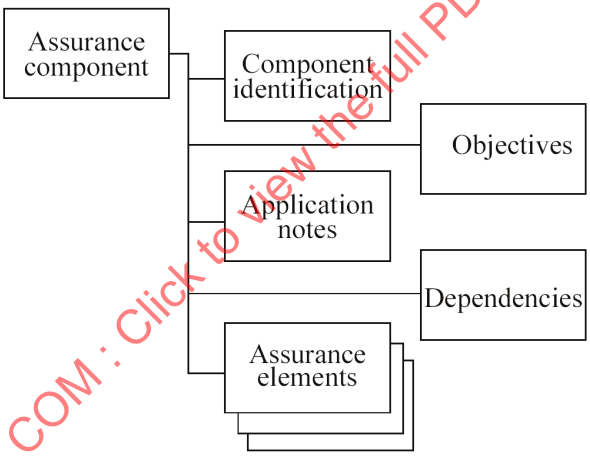


Figure 2 - Assurance component structure

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.

6.1.3.1 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,

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

followed by a period, and then a numeric character. The numeric characters for the components within each family are assigned sequentially, starting from 1.

6.1.3.2 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.

6.1.3.3 Application notes

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

6.1.3.4 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.

6.1.3.5 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 ISO/IEC 15408.

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, and, when considered appropriate, specific characteristics that either the TOE or this assurance must possess. 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 requirements. 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

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: Protection Profile evaluation and ASE: Security Target evaluation in clauses 8 and 9. 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.

6.1.4 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*.

6.1.5 EAL structure

Figure 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

Part 3 Assurance levels

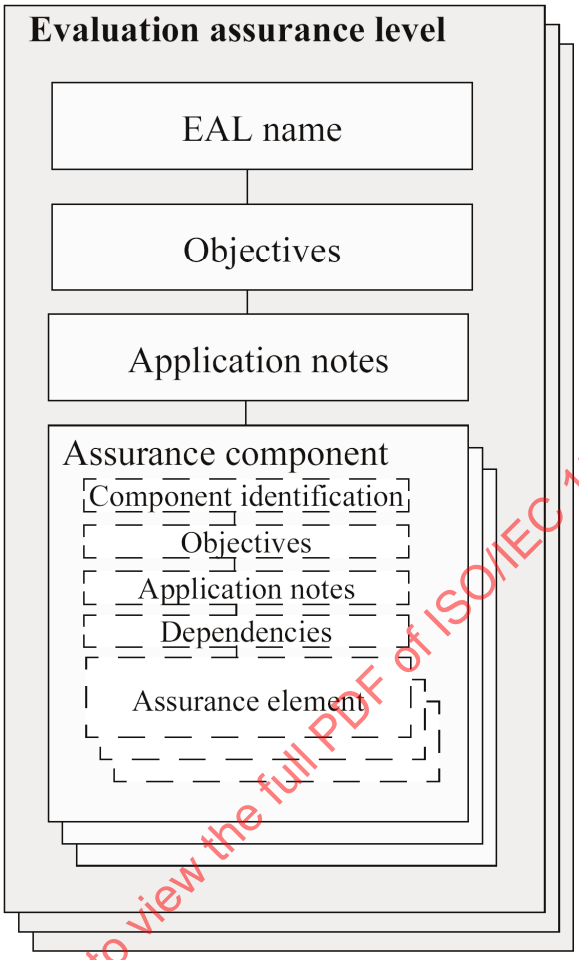


Figure 3 - EAL structure

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

6.1.5.1 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.

6.1.5.2 Objectives

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

6.1.5.3 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.

6.1.5.3.1 Assurance components

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

© ISO/IEC 2005 - All rights reserved

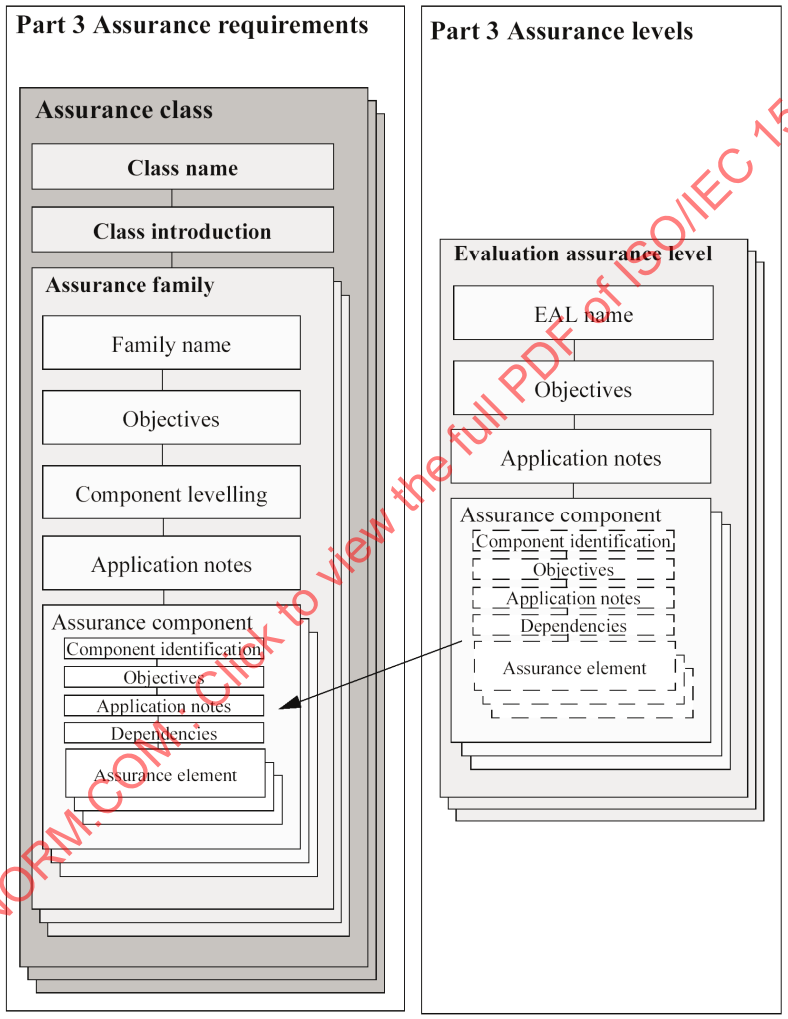
A higher level of assurance than that provided by a given EAL can be achieved by:

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.

6.1.5.4 Relationship between assurances and assurance levels

Figure 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.



IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

Figure 4 - Assurance and assurance level association

6.2 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.

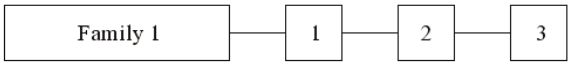


Figure 5 - Sample class decomposition diagram

© ISO/IEC 2005 - All rights reserved

In Figure 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.

6.3 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 2, 3, 4 and 5 in clause 7 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 A, whereas narrative summaries for the ASE families can be found in ISO/IEC 15408-1, annex B.

6.4 Usage of terms in this part of ISO/IEC 15408

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 ISO/IEC 15408-1 Clause 2 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.

6.4.1
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.

6.4.2
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.

6.4.3
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.

6.4.4
consistent
this term describes a relationship between two or more entities, indicating that there are no apparent contradictions between these entitieAssurance categorisations.

6.4.5
counter (verb)
this term is typically used in the context that the impact of a particular threat is mitigated but not necessarily eradicated.

6.4.6
demonstrate
this term refers to an analysis leading to a conclusion, which is less rigourous than a “proof”.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

6.4.7
describe
this term requires that certain, specific details of an entity be provided.

6.4.8
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.

6.4.9
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.

6.4.10
exhaustive
this term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is reAssurance categorisationlated 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.

6.4.11
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.

6.4.12
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.

6.4.13
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.

6.4.14
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.

6.4.15
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.

6.4.16
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”.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

6.4.17
trace (verb)
this term is used to indicate that an informal correspondence is required between two entities with only a minimal level of rigour.

6.4.18
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.

6.5 Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in Table 1.

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

Table 1 Assurance family breakdown and mapping

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

6.6 Assurance class and family overview

The following summarises the assurance classes and families of clauses 12-18. These classes and family summaries are presented in the same order as they appear in clauses 12-18.

6.6.1 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.

© ISO/IEC 2005 - All rights reserved

6.6.1.1 CM automation (ACM_AUT)

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

6.6.1.2 CM capabilities (ACM_CAP)

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

6.6.1.3 CM scope (ACM_SCP)

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

6.6.2 Class ADO:Delivery and operation

Assurance class ADO: Delivery and operation 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.

6.6.2.1 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.

6.6.2.2 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.

6.6.3 Class ADV:Development

Assurance class ADV: Development 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.

6.6.3.1 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.

6.6.3.2 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.

6.6.3.3 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

6.6.3.4 TSF internals (ADV_INT)

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

6.6.3.5 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.

6.6.3.6 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.

6.6.3.7 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.

6.6.4 Class AGD:Guidance documents

Assurance class AGD: Guidance documents 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.

6.6.4.1 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.

6.6.4.2 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.

6.6.5 Class ALC:Life cycle support

Assurance class ALC: Life cycle support 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.

6.6.5.1 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

6.6.5.2 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.

6.6.5.3 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.

6.6.5.4 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.

6.6.6 Class APE: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.

6.6.7 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.

6.6.8 Class ATE:Tests

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

6.6.8.1 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.

6.6.8.2 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.

6.6.8.3 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

6.6.8.4 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.

6.6.9 Class AVA:Vulnerability assessment

Assurance class AVA: Vulnerability assessment 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.

6.6.9.1 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.

6.6.9.2 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.

6.6.9.3 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.

6.6.9.4 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

7 Protection Profile and Security Target evaluation criteria

7.1 Overview

This clause introduces the evaluation criteria for PPs and STs. The evaluation criteria are then fully presented in clause 8, and clause 9.

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 12 through 18, they are presented in a similar manner because the developer and evaluator activities are comparable for PP, ST and TOE evaluations.

© ISO/IEC 2005 - All rights reserved

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 A and B 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.

7.2 Protection Profile criteria overview

7.2.1 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.

7.2.2 Relation to the Security Target evaluation criteria

As described in annexes A and B 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.

7.2.3 Evaluator tasks

7.2.3.1 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: Protection Profile evaluation class as described in Table 2.

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

Table 2 Protection Profile families - only ISO/IEC 15408 requirements

7.2.3.2 Evaluator tasks for an ISO/IEC 15408 extended evaluation

Evaluators performing a PP evaluation that includes requirements from outside the standard shall apply the requirements of the APE: Protection Profile evaluation class as described in Table 3.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

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

Table 3 Protection Profile families - ISO/IEC 15408 extended requirements

7.3 Security Target criteria overview

7.3.1 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.

7.3.2 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 9 while the requirements for TOE evaluations are contained in clauses 12 through 18.

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.

7.3.3 Evaluator tasks

7.3.3.1 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: Security Target evaluation class as described in Table 4.

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

Table 4 Security Target families - only ISO/IEC 15408 requirements

7.3.3.2 Evaluator tasks for an ISO/IEC 15408 extended evaluation

Evaluators performing an ST evaluation that includes requirements from outside the standard shall apply the requirements of the ASE: Security Target evaluation class as described in Table 5.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

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

Table 5 Security Target families - ISO/IEC 15408 extended requirements

8 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 6 shows the families within this class, and the hierarchy of components within the families.

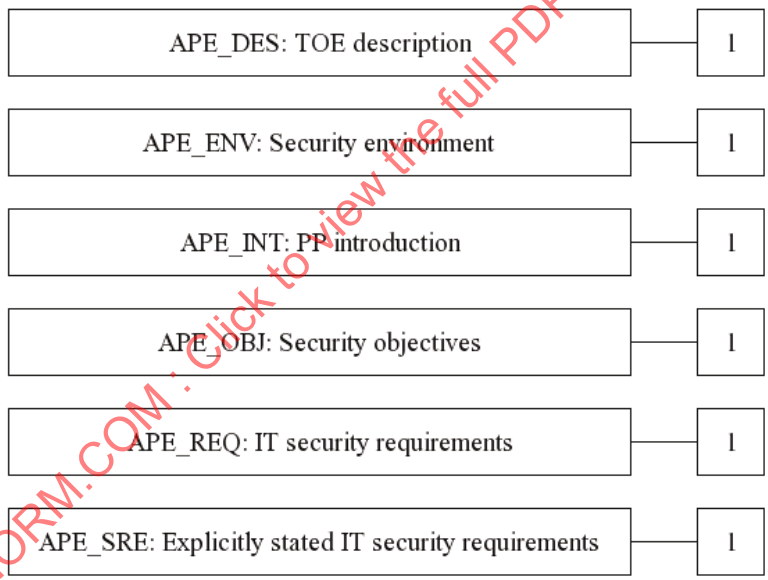


Figure 6 - APE: Protection Profile evaluation class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

8.1 TOE description (APE_DES)

8.1.1 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.

© ISO/IEC 2005 - All rights reserved

8.1.2 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

8.1.2.1 Developer action elements

8.1.2.1.1 APE_DES.1.1D

The PP developer shall provide a TOE description as part of the PP.

8.1.2.2 Content and presentation of evidence elements

8.1.2.2.1 APE_DES.1.1C

The TOE description shall describe the product type and the general IT features of the TOE.

8.1.2.3 Evaluator action elements

8.1.2.3.1 APE_DES.1.1E

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

8.1.2.3.2 APE_DES.1.2E

The evaluator shall confirm that the TOE description is coherent and internally consistent.

8.1.2.3.3 APE_DES.1.3E

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

8.2 Security environment (APE_ENV)

8.2.1 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.

8.2.2 APE_ENV.1 Protection Profile, Security environment, Evaluation requirements

Dependencies: No dependencies.

8.2.2.1 Developer action elements

8.2.2.1.1 APE_ENV.1.1D

The PP developer shall provide a statement of TOE security environment as part of the PP.

8.2.2.2 Content and presentation of evidence elements

8.2.2.2.1 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

8.2.2.2.2 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.

8.2.2.2.3 APE_ENV.1.3C

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

8.2.2.3 Evaluator action elements

8.2.2.3.1 APE_ENV.1.1E

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

8.2.2.3.2 APE_ENV.1.2E

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

8.3 PP introduction (APE_INT)

8.3.1 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.

8.3.2 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

8.3.2.1 Developer action elements

8.3.2.1.1 APE_INT.1.1D

The PP developer shall provide a PP introduction as part of the PP.

8.3.2.2 Content and presentation of evidence elements

8.3.2.2.1 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.

8.3.2.2.2 APE_INT.1.2C

The PP introduction shall contain a PP overview which summarises the PP in narrative form.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

8.3.2.3 Evaluator action elements

8.3.2.3.1 APE_INT.1.1E

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

8.3.2.3.2 APE_INT.1.2E

The evaluator shall confirm that the PP introduction is coherent and internally consistent.

8.3.2.3.3 APE_INT.1.3E

The evaluator shall confirm that the PP introduction is consistent with the other parts of the PP.

8.4 Security objectives (APE_OBJ)

8.4.1 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.

8.4.2 APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

Dependencies: APE_ENV.1 Protection Profile, Security environment, Evaluation requirements

8.4.2.1 Developer action elements

8.4.2.1.1 APE_OBJ.1.1D

The PP developer shall provide a statement of security objectives as part of the PP.

8.4.2.1.2 APE_OBJ.1.2D

The PP developer shall provide the security objectives rationale.

8.4.2.2 Content and presentation of evidence elements

8.4.2.2.1 APE_OBJ.1.1C

The statement of security objectives shall define the security objectives for the TOE and its environment.

8.4.2.2.2 APE_OBJ.1.2C

The security objectives for the TOE shall be 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.

8.4.2.2.3 APE_OBJ.1.3C

The security objectives for the environment shall be 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

8.4.2.2.4 APE_OBJ.1.4C

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

8.4.2.2.5 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.

8.4.2.3 Evaluator action elements

8.4.2.3.1 APE_OBJ.1.1E

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

8.4.2.3.2 APE_OBJ.1.2E

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

8.5 IT security requirements (APE_REQ)

8.5.1 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 Explicitly stated IT security requirements (APE_SRE) family.

8.5.2 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 Protection Profile, IT security requirements, Evaluation requirements 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 A.

ISO/IEC 15408 recognises the validity of multiple SOF domains within a given TOE. A SOF domain is a subset of the TOE (logical or physical) for which a specific functional strength level is appropriate, in the context of the intended environment. This allows for a TOE with some functionality having a higher minimum strength requirement than other functionality. For a TOE with multiple SOF domains, the phrase “minimum strength of function” is used to indicate the set that contains the minimum strength of function for each domain,

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

identified by domain. Additionally, the requirements rationale must consider the SOF level for each domain in light of how that that domain impacts meeting the security objectives.

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

Dependencies: APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

8.5.3.1 Developer action elements

8.5.3.1.1 APE_REQ.1.1D

The PP developer shall provide a statement of IT security requirements as part of the PP.

8.5.3.1.2 APE_REQ.1.2D

The PP developer shall provide the security requirements rationale.

8.5.3.2 Content and presentation of evidence elements

8.5.3.2.1 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.

8.5.3.2.2 APE_REQ.1.2C

The statement of TOE security assurance requirements shall identify the TOE security assurance requirements drawn from this part of ISO/IEC 15408 assurance requirements components.

8.5.3.2.3 APE_REQ.1.3C

The statement of TOE security assurance requirements should include an Evaluation Assurance Level (EAL) as defined in this part of ISO/IEC 15408.

8.5.3.2.4 APE_REQ.1.4C

The evidence shall justify that the statement of TOE security assurance requirements is appropriate.

8.5.3.2.5 APE_REQ.1.5C

The PP shall, if appropriate, identify any security requirements for the IT environment.

8.5.3.2.6 APE_REQ.1.6C

All completed operations on IT security requirements included in the PP shall be identified.

8.5.3.2.7 APE_REQ.1.7C

Any uncompleted operations on IT security requirements included in the PP shall be identified.

8.5.3.2.8 APE_REQ.1.8C

Dependencies among the IT security requirements included in the PP should be satisfied.

8.5.3.2.9 APE_REQ.1.9C

The evidence shall justify why any non-satisfaction of dependencies is appropriate.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

8.5.3.2.10 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.

8.5.3.2.11 APE_REQ.1.11C

The statement of security requirements shall identify all security functional requirements for which an explicit strength of function claim is required, together with the explicit strength of function claim for each such security functional requirement.

8.5.3.2.12 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.

8.5.3.2.13 APE_REQ.1.13C

The security requirements rationale shall demonstrate that the IT security requirements are suitable to meet the security objectives.

8.5.3.2.14 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.

8.5.3.3 Evaluator action elements

8.5.3.3.1 APE_REQ.1.1E

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

8.5.3.3.2 APE_REQ.1.2E

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

8.6 Explicitly stated IT security requirements (APE_SRE)

8.6.1 Objectives

If, after careful consideration, none of the requirements components in ISO/IEC 15408-2 or this part of ISO/IEC 15408 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 IT security requirements (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.

8.6.2 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

Using 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”.

The elements APE_SRE.1.5C and APE_SRE.1.6C require that the explicitly stated IT security requirements shall be measurable and objective as well as clearly and unambiguously expressed. The existing ISO/IEC 15408 functional and assurance requirements are to be used as models for compliance with these requirements.

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

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

8.6.3.1 Developer action elements

8.6.3.1.1 APE_SRE.1.1D

The PP developer shall provide a statement of IT security requirements as part of the PP.

8.6.3.1.2 APE_SRE.1.2D

The PP developer shall provide the security requirements rationale.

8.6.3.2 Content and presentation of evidence elements

8.6.3.2.1 APE_SRE.1.1C

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

8.6.3.2.2 APE_SRE.1.2C

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

8.6.3.2.3 APE_SRE.1.3C

The evidence shall justify why the security requirements had to be explicitly stated.

8.6.3.2.4 APE_SRE.1.4C

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

8.6.3.2.5 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

8.6.3.2.6 APE_SRE.1.6C

The explicitly stated IT security requirements shall be clearly and unambiguously expressed.

8.6.3.2.7 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.

8.6.3.3 Evaluator action elements

8.6.3.3.1 APE_SRE.1.1E

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

8.6.3.3.2 APE_SRE.1.2E

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

9 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 7 shows the families within this class, and the hierarchy of components within the families.

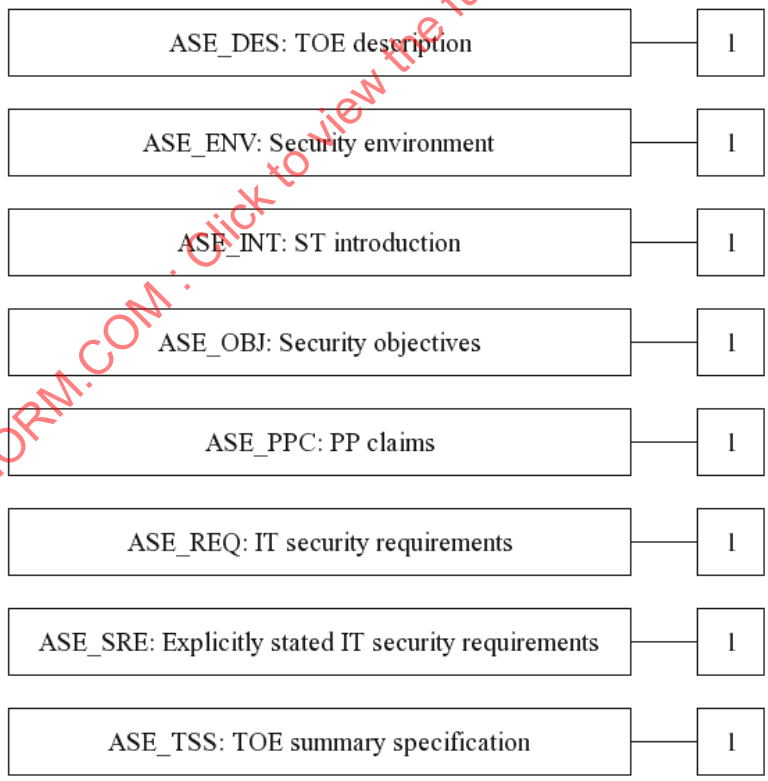


Figure 7 - ASE: Security Target evaluation class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.1 TOE description (ASE_DES)

9.1.1 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.

9.1.2 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

9.1.2.1 Developer action elements

9.1.2.1.1 ASE_DES.1.1D

The developer shall provide a TOE description as part of the ST.

9.1.2.2 Content and presentation of evidence elements

9.1.2.2.1 ASE_DES.1.1C

The TOE description shall 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 .

9.1.2.3 Evaluator action elements

9.1.2.3.1 ASE_DES.1.1E

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

9.1.2.3.2 ASE_DES.1.2E

The evaluator shall confirm that the TOE description is coherent and internally consistent.

9.1.2.3.3 ASE_DES.1.3E

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

9.2 Security environment (ASE_ENV)

9.2.1 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.2.2 ASE_ENV.1 Security Target, Security environment, Evaluation requirements

Dependencies: No dependencies.

9.2.2.1 Developer action elements

9.2.2.1.1 ASE_ENV.1.1D

The developer shall provide a statement of TOE security environment as part of the ST.

9.2.2.2 Content and presentation of evidence elements

9.2.2.2.1 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.

9.2.2.2.2 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.

9.2.2.2.3 ASE_ENV.1.3C

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

9.2.2.3 Evaluator action elements

9.2.2.3.1 ASE_ENV.1.1E

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

9.2.2.3.2 ASE_ENV.1.2E

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

9.3 ST introduction (ASE_INT)

9.3.1 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.

9.3.2 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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.3.2.1 Developer action elements

9.3.2.1.1 ASE_INT.1.1D

The developer shall provide an ST introduction as part of the ST.

9.3.2.2 Content and presentation of evidence elements

9.3.2.2.1 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.

9.3.2.2.2 ASE_INT.1.2C

The ST introduction shall contain an ST overview which summarises the ST in narrative form.

9.3.2.2.3 ASE_INT.1.3C

The ST introduction shall contain an ISO/IEC 15408 conformance claim that states any evaluatable claim of ISO/IEC 15408 conformance for the TOE.

9.3.2.3 Evaluator action elements

9.3.2.3.1 ASE_INT.1.1E

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

9.3.2.3.2 ASE_INT.1.2E

The evaluator shall confirm that the ST introduction is coherent and internally consistent.

9.3.2.3.3 ASE_INT.1.3E

The evaluator shall confirm that the ST introduction is consistent with the other parts of the ST.

9.4 Security objectives (ASE_OBJ)

9.4.1 Objectives

The security objectives are 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.

9.4.2 ASE_OBJ.1 Security Target, Security objectives, Evaluation requirements

Dependencies: ASE_ENV.1 Security Target, Security environment, Evaluation requirements

9.4.2.1 Developer action elements

9.4.2.1.1 ASE_OBJ.1.1D

The developer shall provide a statement of security objectives as part of the ST.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.4.2.1.2 ASE_OBJ.1.2D

The developer shall provide the security objectives rationale.

9.4.2.2 Content and presentation of evidence elements

9.4.2.2.1 ASE_OBJ.1.1C

The statement of security objectives shall define the security objectives for the TOE and its environment.

9.4.2.2.2 ASE_OBJ.1.2C

The security objectives for the TOE shall be 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.

9.4.2.2.3 ASE_OBJ.1.3C

The security objectives for the environment shall be 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.

9.4.2.2.4 ASE_OBJ.1.4C

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

9.4.2.2.5 ASE_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.

9.4.2.3 Evaluator action elements

9.4.2.3.1 ASE_OBJ.1.1E

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

9.4.2.3.2 ASE_OBJ.1.2E

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

9.5 PP claims (ASE_PPC)

9.5.1 Objectives

The goal of the evaluation of the Security Target PP claims is to determine whether the ST is a correct instantiation of the PP.

9.5.2 Application notes

The family applies only in the case of a PP claim. In all other cases, no developer action and no evaluator action is necessary.

Although additional evaluation activity is necessary when a PP claim is made, the ST evaluation effort is generally smaller than in cases where no PP is used because it is possible to reuse the PP evaluation results for the ST evaluation.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.5.3 ASE_PPC.1 Security Target, PP claims, Evaluation requirements

Dependencies: ASE_OBJ.1 Security Target, Security objectives, Evaluation requirements

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

9.5.3.1 Developer action elements

9.5.3.1.1 ASE_PPC.1.1D

The developer shall provide any PP claims as part of the ST.

9.5.3.1.2 ASE_PPC.1.2D

The developer shall provide the PP claims rationale for each provided PP claim.

9.5.3.2 Content and presentation of evidence elements

9.5.3.2.1 ASE_PPC.1.1C

Each PP claim shall identify the PP for which compliance is being claimed, including qualifications needed for that claim.

9.5.3.2.2 ASE_PPC.1.2C

Each PP claim shall identify the IT security requirements statements that satisfy the permitted operations of the PP or otherwise further qualify the PP requirements.

9.5.3.2.3 ASE_PPC.1.3C

Each PP claim shall identify security objectives and IT security requirements statements contained in the ST that are in addition to those contained in the PP.

9.5.3.3 Evaluator action elements

9.5.3.3.1 ASE_PPC.1.1E

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

9.5.3.3.2 ASE_PPC.1.2E

The evaluator shall confirm that the PP claims are a correct instantiation of the PP.

9.6 IT security requirements (ASE_REQ)

9.6.1 Objectives

The IT security requirements chosen for a TOE and presented or cited in an ST 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.

This family presents evaluation requirements that permit the evaluator to determine that an ST is suitable for use as a statement of requirements for the corresponding TOE. The additional criteria necessary for the evaluation of explicitly stated requirements is covered in the Explicitly stated IT security requirements (ASE_SRE) family.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.6.2 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 ASE_REQ.1 Security Target, IT security requirements, Evaluation requirements 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 ST. Detailed information for all these aspects is contained in ISO/IEC 15408-1, annex B.

ISO/IEC 15408 recognises the validity of multiple SOF domains within a given TOE. A SOF domain is a subset of the TOE (logical or physical) for which a specific functional strength level is appropriate, in the context of the intended environment. This allows for a TOE with some functionality having a higher minimum strength requirement than other functionality. For a TOE with multiple SOF domains, the phrase “minimum strength of function” is used to indicate the set that contains the minimum strength of function for each domain, identified by domain. Additionally, the requirements rationale must consider the SOF level for each domain in light of how that that domain impacts meeting the security objectives.

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

Dependencies: ASE_OBJ.1 Security Target, Security objectives, Evaluation requirements

9.6.3.1 Developer action elements

9.6.3.1.1 ASE_REQ.1.1D

The developer shall provide a statement of IT security requirements as part of the ST.

9.6.3.1.2 ASE_REQ.1.2D

The developer shall provide the security requirements rationale.

9.6.3.2 Content and presentation of evidence elements

9.6.3.2.1 ASE_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.

9.6.3.2.2 ASE_REQ.1.2C

The statement of TOE security assurance requirements shall identify the TOE security assurance requirements drawn from this part of ISO/IEC 15408 assurance requirements components.

9.6.3.2.3 ASE_REQ.1.3C

The statement of TOE security assurance requirements should include an Evaluation Assurance Level (EAL) as defined in this part of ISO/IEC 15408.

9.6.3.2.4 ASE_REQ.1.4C

The evidence shall justify that the statement of TOE security assurance requirements is appropriate.

9.6.3.2.5 ASE_REQ.1.5C

The ST shall, if appropriate, identify any security requirements for the IT environment.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.6.3.2.6 ASE_REQ.1.6C

Operations on IT security requirements included in the ST shall be identified and performed.

9.6.3.2.7 ASE_REQ.1.7C

Dependencies among the IT security requirements included in the ST should be satisfied.

9.6.3.2.8 ASE_REQ.1.8C

The evidence shall justify why any non-satisfaction of dependencies is appropriate.

9.6.3.2.9 ASE_REQ.1.9C

The ST 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.

9.6.3.2.10 ASE_REQ.1.10C

The statement of security requirements shall identify all security functional requirements for which an explicit strength of function claim is required, together with the explicit strength of function claim for each such security functional requirement.

9.6.3.2.11 ASE_REQ.1.11C

The security requirements rationale shall demonstrate that the minimum strength of function level for the ST together with any explicit strength of function claim is consistent with the security objectives for the TOE.

9.6.3.2.12 ASE_REQ.1.12C

The security requirements rationale shall demonstrate that the IT security requirements are suitable to meet the security objectives.

9.6.3.2.13 ASE_REQ.1.13C

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

9.6.3.3 Evaluator action elements

9.6.3.3.1 ASE_REQ.1.1E

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

9.6.3.3.2 ASE_REQ.1.2E

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

9.7 Explicitly stated IT security requirements (ASE_SRE)

9.7.1 Objectives

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

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 IT security requirements (ASE_REQ) family.

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

9.7.2 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 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”.

The elements ASE_SRE.1.5C and ASE_SRE.1.6C require that the explicitly stated IT security requirements shall be measurable and objective as well as clearly and unambiguously expressed. The existing ISO/IEC 15408 functional and assurance requirements are to be used as models for compliance with these requirements.

9.7.3 ASE_SRE.1 Security Target, Explicitly stated IT security requirements, Evaluation requirements

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

9.7.3.1 Developer action elements

9.7.3.1.1 ASE_SRE.1.1D

The developer shall provide a statement of IT security requirements as part of the ST.

9.7.3.1.2 ASE_SRE.1.2D

The developer shall provide the security requirements rationale.

9.7.3.2 Content and presentation of evidence elements

9.7.3.2.1 ASE_SRE.1.1C

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

9.7.3.2.2 ASE_SRE.1.2C

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

9.7.3.2.3 ASE_SRE.1.3C

The evidence shall justify why the security requirements had to be explicitly stated.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.7.3.2.4 ASE_SRE.1.4C

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

9.7.3.2.5 ASE_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.

9.7.3.2.6 ASE_SRE.1.6C

The explicitly stated IT security requirements shall be clearly and unambiguously expressed.

9.7.3.2.7 ASE_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.

9.7.3.3 Evaluator action elements

9.7.3.3.1 ASE_SRE.1.1E

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

9.7.3.3.2 ASE_SRE.1.2E

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

9.8 TOE summary specification (ASE_TSS)

9.8.1 Objectives

The TOE summary specification provides a high-level definition of the security functions claimed to meet the functional requirements and of the assurance measures taken to meet the assurance requirements.

9.8.2 Application notes

The relationship between the IT security functions and the TOE security functional requirements can be a “many to many” relationship. Nevertheless, every security function shall contribute to the satisfaction of at least one security requirement in order to be able to clearly define the TSF. Security functions that do not fulfil this requirement should normally not be necessary. Note, however, that the requirement that a security function contributes to the satisfaction of at least one security requirement is worded in a quite general manner, so that all the security functions found to be useful for the TOE should be justifiable.

The statement of assurance measures is of specific relevance in all those cases where assurance requirements not taken from ISO/IEC 15408 are included in the ST. If the TOE security assurance requirements in the ST are exclusively based on ISO/IEC 15408 evaluation assurance levels or other this part of ISO/IEC 15408 assurance components, then the assurance measures could be presented in the form of a reference to the documents that show that the assurance requirements are met.

In the ASE_TSS.1 Security Target, TOE summary specification, Evaluation requirements 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 ST. Detailed information for all these aspects is contained in ISO/IEC 15408-1, annex B.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

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

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

9.8.3.1 Developer action elements

9.8.3.1.1 ASE_TSS.1.1D

The developer shall provide a TOE summary specification as part of the ST.

9.8.3.1.2 ASE_TSS.1.2D

The developer shall provide the TOE summary specification rationale.

9.8.3.2 Content and presentation of evidence elements

9.8.3.2.1 ASE_TSS.1.1C

The TOE summary specification shall describe the IT security functions and the assurance measures of the TOE.

9.8.3.2.2 ASE_TSS.1.2C

The TOE summary specification shall trace the IT security functions to the TOE security functional requirements such that it can be seen which IT security functions satisfy which TOE security functional requirements and that every IT security function contributes to the satisfaction of at least one TOE security functional requirement.

9.8.3.2.3 ASE_TSS.1.3C

The IT security functions shall be defined in an informal style to a level of detail necessary for understanding their intent.

9.8.3.2.4 ASE_TSS.1.4C

All references to security mechanisms included in the ST shall be traced to the relevant security functions so that it can be seen which security mechanisms are used in the implementation of each function.

9.8.3.2.5 ASE_TSS.1.5C

The TOE summary specification rationale shall demonstrate that the IT security functions are suitable to meet the TOE security functional requirements.

9.8.3.2.6 ASE_TSS.1.6C

The TOE summary specification rationale shall demonstrate that the combination of the specified IT security functions work together so as to satisfy the TOE security functional requirements.

9.8.3.2.7 ASE_TSS.1.7C

The TOE summary specification shall trace the assurance measures to the assurance requirements so that it can be seen which measures contribute to the satisfaction of which requirements.

9.8.3.2.8 ASE_TSS.1.8C

The TOE summary specification rationale shall demonstrate that the assurance measures meet all assurance requirements of the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

9.8.3.2.9 ASE_TSS.1.9C

The TOE summary specification shall identify all IT security functions that are realised by a probabilistic or permutational mechanism, as appropriate.

9.8.3.2.10 ASE_TSS.1.10C

The TOE summary specification shall, for each IT security function for which it is appropriate, state the strength of function claim either as a specific metric, or as SOF-basic, SOF-medium or SOF-high.

9.8.3.3 Evaluator action elements

9.8.3.3.1 ASE_TSS.1.1E

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

9.8.3.3.2 ASE_TSS.1.2E

The evaluator shall confirm that the TOE summary specification is complete, coherent, and internally consistent.

10 Evaluation assurance levels

The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. ISO/IEC 15408 approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from this part of ISO/IEC 15408 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

10.1 Evaluation assurance level (EAL) overview

Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next subclause, seven hierarchically ordered evaluation assurance levels are defined in ISO/IEC 15408 for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in clause 6 of this part of ISO/IEC 15408. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in ISO/IEC 15408, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in ISO/IEC 15408, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	**3**
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Table 6 Evaluation assurance level summary

10.2 Evaluation assurance level details

The following subclauses provide definitions of the EALs, highlighting differences between the specific requirements and the prose characterisations of those requirements using bold type.

10.3 Evaluation assurance level 1 (EAL1) - functionally tested

10.3.1 Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

10.3.2 Assurance components

EAL1 provides a basic level of assurance by an analysis of the security functions using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by independent testing of the TOE security functions.

This EAL provides a meaningful increase in assurance over an unevaluated IT product or system.

Assurance Class	Assurance components
ACM: Configuration management	ACM_CAP.1 Version numbers
ADO: Delivery and operation	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_RCR.1 Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ATE: Tests	ATE_IND.1 Independent testing - conformance

Table 7 EAL1

10.4 Evaluation assurance level 2 (EAL2) - structurally tested

10.4.1 Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

10.4.2 Assurance components

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis, and independent testing based upon more detailed TOE specifications.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

Assurance Class	Assurance components
ACM: Configuration management	ACM_CAP.2 Configuration items
ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 8 EAL2

10.5 Evaluation assurance level 3 (EAL3) - methodically tested and checked

10.5.1 Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.

10.5.2 Assurance components

EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

EAL3 also provides assurance through the use of development environment controls, TOE configuration management, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL2 by requiring more complete testing coverage of the security functions and mechanisms and/or procedures that provide some confidence that the TOE will not be tampered with during development.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

Assurance Class	Assurance components
ACM: Configuration management	ACM_CAP.3 Authorisation controls
	ACM_SCP.1 TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.1 Identification of security measures
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 9 EAL3

10.6 Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed

10.6.1 Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

10.6.2 Assurance components

EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, a subset of the implementation, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development or delivery.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

Assurance Class	Assurance components
ACM: Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

Table 10 EAL4

10.7 Evaluation assurance level 5 (EAL5) - semiformally designed and tested

10.7.1 Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

10.7.2 Assurance components

EAL5 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and all of the implementation, to understand the security behaviour. Assurance is additionally gained through a formal model of the TOE security policy and a semiformal presentation of the functional specification and high-level design and a semiformal demonstration of correspondence between them. A modular TOE design is also required.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, high-level design and low-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a moderate attack potential. The analysis also includes validation of the developer's covert channel analysis.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

EAL5 also provides assurance through the use of a development environment controls, and comprehensive TOE configuration management including automation, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, the entire implementation, a more structured (and hence analysable) architecture, covert channel analysis, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

Assurance Class	Assurance components
ACM: Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.3 Development tools CM coverage
ADO: Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.3 Semiformal functional specification
	ADV_HLD.3 Semiformal high-level design
	ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Modularity
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.2 Semiformal correspondence demonstration
	ADV_SPM.3 Formal TOE security policy model
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_LCD.2 Standardised life-cycle model
	ALC_TAT.2 Compliance with implementation standards
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: low-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_CCA.1 Covert channel analysis
	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.3 Moderately resistant

Table 11 EAL5

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

10.8 Evaluation assurance level 6 (EAL6) - semiformally verified design and tested

10.8.1 Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.

10.8.2 Assurance components

EAL6 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the of the TOE, and a structured presentation of the implementation, to understand the security behaviour. Assurance is additionally gained through a formal model of the TOE security policy, a semiformal presentation of the functional specification, high-level design, and low-level design and a semiformal demonstration of correspondence between them. A modular and layered TOE design is also required.

© ISO/IEC 2005 - All rights reserved

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, high-level design and low-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential. The analysis also includes validation of the developer's systematic covert channel analysis.

EAL6 also provides assurance through the use of a structured development process, development environment controls, and comprehensive TOE configuration management including complete automation, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL5 by requiring more comprehensive analysis, a structured representation of the implementation, more architectural structure (e.g. layering), more comprehensive independent vulnerability analysis, systematic covert channel identification, and improved configuration management and development environment controls.

Assurance Class	Assurance components
ACM: Configuration management	ACM_AUT.2 Complete CM automation
	ACM_CAP.5 Advanced support
	ACM_SCP.3 Development tools CM coverage
ADO: Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.3 Semiformal functional specification
	ADV_HLD.4 Semiformal high-level explanation
	ADV_IMP.3 Structured implementation of the TSF
	ADV_INT.2 Reduction of complexity
	ADV_LLD.2 Semiformal low-level design
	ADV_RCR.2 Semiformal correspondence demonstration
	ADV_SPM.3 Formal TOE security policy model
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.2 Standardised life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.2 Testing: low-level design
	ATE_FUN.2 Ordered functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_CCA.2 Systematic covert channel analysis
	AVA_MSU.3 Analysis and testing for insecure states
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.4 Highly resistant

Table 12 EAL6

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

10.9 Evaluation assurance level 7 (EAL7) - formally verified design and tested

10.9.1 Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

10.9.2 Assurance components

EAL7 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a structured presentation of the implementation, to understand the security behaviour. Assurance is additionally gained

© ISO/IEC 2005 - All rights reserved

through a formal model of the TOE security policy, a formal presentation of the functional specification and high-level design, a semiformal presentation of the low-level design, and formal and semiformal demonstration of correspondence between them, as appropriate. A modular, layered and simple TOE design is also required.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification high-level design, low-level design and implementation representation, complete independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential. The analysis also includes validation of the developer's systematic covert channel analysis.

EAL7 also provides assurance through the use of a structured development process, development environment controls, and comprehensive TOE configuration management including complete automation, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL6 by requiring more comprehensive analysis using formal representations and formal correspondence, and comprehensive testing.

Assurance Class	Assurance components
ACM: Configuration management	ACM_AUT.2 Complete CM automation
	ACM_CAP.5 Advanced support
	ACM_SCP.3 Development tools CM coverage
ADO: Delivery and operation	ADO_DEL.3 Prevention of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.4 Formal functional specification
	ADV_HLD.5 Formal high-level design
	ADV_IMP.3 Structured implementation of the TSF
	ADV_INT.3 Minimisation of complexity
	ADV_LLD.2 Semiformal low-level design
	ADV_RCR.3 Formal correspondence demonstration
	ADV_SPM.3 Formal TOE security policy model
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.3 Measurable life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.3 Testing: implementation representation
	ATE_FUN.2 Ordered functional testing
	ATE_IND.3 Independent testing - complete
AVA: Vulnerability assessment	AVA_CCA.2 Systematic covert channel analysis
	AVA_MSU.3 Analysis and testing for insecure states
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.4 Highly resistant

Table 13 EAL7

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

11 Assurance classes, families, and components

The next seven clauses provide the detailed requirements, presented in alphabetical order, of each of the assurance components, grouped by class and family.

12 Class ACM: Configuration management

Configuration management (CM) is one method or means for establishing that the functional requirements and specifications are realised in the implementation of the TOE. CM meets these objectives by requiring discipline and control in the processes of refinement and modification of the TOE and the related information.

© ISO/IEC 2005 - All rights reserved

CM systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorised.

Figure 8 shows the families within this class, and the hierarchy of components within the families.

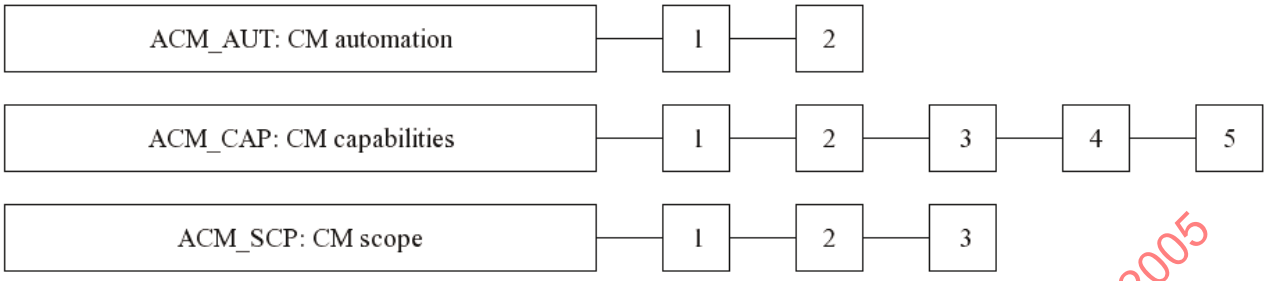


Figure 8 - ACM: Configuration management class decomposition

12.1 CM automation (ACM_AUT)

12.1.1 Objectives

The objective of introducing automated CM tools is to increase the effectiveness of the CM system. While both automated and manual CM systems can be bypassed, ignored, or prove insufficient to prevent unauthorised modification, automated systems are less susceptible to human error or negligence.

12.1.2 Component levelling

The components in this family are levelled on the basis of the set of configuration items that are controlled through automated means.

12.1.3 Application notes

ACM_AUT.1.1C introduces a requirement that is related to the implementation representation of the TOE. The implementation representation of the TOE consists of all hardware, software, and firmware that comprise the physical TOE. In the case of a software-only TOE, the implementation representation may consist solely of source and object code.

ACM_AUT.1.2C introduces a requirement that the CM system provide an automated means to support the generation of the TOE. This requires that the CM system provide an automated means to assist in determining that the correct configuration items are used in generating the TOE.

ACM_AUT.2.5C introduces a requirement that the CM system provide an automated means to ascertain the changes between the TOE and its preceding version. If no previous version of the TOE exists, the developer still needs to provide an automated means to ascertain the changes between the TOE and a future version of the TOE.

12.1.4 ACM_AUT.1 Partial CM automation

Dependencies: ACM_CAP.3 Authorisation controls

12.1.4.1 Objectives

In development environments where the implementation representation is complex or is being developed by multiple developers, it is difficult to control changes without the support of automated tools. In particular, these automated tools need to be able to support the numerous changes that occur during development and ensure that those changes are authorised. It is the objective of this component to ensure that the implementation representation is controlled through automated means.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.1.4.2 Developer action elements

12.1.4.2.1 ACM_AUT.1.1D

The developer shall use a CM system.

12.1.4.2.2 ACM_AUT.1.2D

The developer shall provide a CM plan.

12.1.4.3 Content and presentation of evidence elements

12.1.4.3.1 ACM_AUT.1.1C

The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

12.1.4.3.2 ACM_AUT.1.2C

The CM system shall provide an automated means to support the generation of the TOE.

12.1.4.3.3 ACM_AUT.1.3C

The CM plan shall describe the automated tools used in the CM system.

12.1.4.3.4 ACM_AUT.1.4C

The CM plan shall describe how the automated tools are used in the CM system.

12.1.4.4 Evaluator action elements

12.1.4.4.1 ACM_AUT.1.1E

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

12.1.5 ACM_AUT.2 Complete CM automation

Dependencies: ACM_CAP.3 Authorisation controls

12.1.5.1 Objectives

In development environments where the configuration items are complex or are being developed by multiple developers, it is difficult to control changes without the support of automated tools. In particular, these automated tools need to be able to support the numerous changes that occur during development and ensure that those changes are authorised. It is the objective of this component to ensure that all configuration items are controlled through automated means.

Providing an automated means of ascertaining changes between versions of the TOE and identifying which configuration items are affected by modifications to other configuration items assists in determining the impact of the changes between successive versions of the TOE. This in turn can provide valuable information in determining whether changes to the TOE result in all configuration items being consistent with one another.

12.1.5.2 Developer action elements

12.1.5.2.1 ACM_AUT.2.1D

The developer shall use a CM system.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.1.5.2.2 ACM_AUT.2.2D

The developer shall provide a CM plan.

12.1.5.3 Content and presentation of evidence elements

12.1.5.3.1 ACM_AUT.2.1C

The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation, **and to all other configuration items.**

12.1.5.3.2 ACM_AUT.2.2C

The CM system shall provide an automated means to support the generation of the TOE.

12.1.5.3.3 ACM_AUT.2.3C

The CM plan shall describe the automated tools used in the CM system.

12.1.5.3.4 ACM_AUT.2.4C

The CM plan shall describe how the automated tools are used in the CM system.

12.1.5.3.5 ACM_AUT.2.5C

The CM system shall provide an automated means to ascertain the changes between the TOE and its preceding version.

12.1.5.3.6 ACM_AUT.2.6C

The CM system shall provide an automated means to identify all other configuration items that are affected by the modification of a given configuration item.

12.1.5.4 Evaluator action elements

12.1.5.4.1 ACM_AUT.2.1E

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

12.2 CM capabilities (ACM_CAP)

12.2.1 Objectives

The capabilities of the CM system address the likelihood that accidental or unauthorised modifications of the configuration items will occur. The CM system should ensure the integrity of the TOE from the early design stages through all subsequent maintenance efforts.

The objectives of this family include the following:

a) ensuring that the TOE is correct and complete before it is sent to the consumer;

b) ensuring that no configuration items are missed during evaluation;

c) preventing unauthorised modification, addition, or deletion of TOE configuration items.

In the case where the TOE is a subset of a product, the ACM requirements apply only to the TOE configuration items, not to the product as a whole. While it is desired that CM be applied from the early design

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

stages and continue into the future, ACM requires that CM be in place and in use prior to the end of the evaluation.

12.2.2 Component levelling

The components in this family are levelled on the basis of the CM system capabilities, the scope of the CM documentation provided by the developer, and whether the developer provides justification that the CM system meets its security requirements.

12.2.3 Application notes

ACM_CAP.2 Configuration items introduces several elements which refer to configuration items. The CM scope (ACM_SCP) family contains requirements for the configuration items to be tracked by the CM system.

ACM_CAP.2.3C introduces a requirement that a configuration list be provided. The configuration list contains all configuration items that are maintained by the CM system.

ACM_CAP.2.7C introduces a requirement that the CM system uniquely identify all configuration items. This also requires that modifications to configuration items result in a new, unique identifier being assigned.

ACM_CAP.3.9C introduces the requirement that the evidence shall demonstrate that the CM system operates in accordance with the CM plan. Examples of such evidence might be documentation such as screen snapshots or audit trail output from the CM system, or a detailed demonstration of the CM system by the developer. The evaluator is responsible for determining that this evidence is sufficient to show that the CM system operates in accordance with the CM plan.

ACM_CAP.3.10C introduces the requirement that evidence be provided to show that all configuration items are being maintained under the CM system. Since a configuration item refers to an item that is on the configuration list, this requirement states that all items on the configuration list are maintained under the CM system.

ACM_CAP.4.12C introduces the requirement that the CM system support the generation of the TOE. This requires that the CM system provide information and/or electronic means to assist in determining that the correct configuration items are used in generating the TOE.

CM capabilities (ACM_CAP) identifies the CM requirements to be imposed on all items identified in the configuration item list. Other than the TOE itself, CM capabilities (ACM_CAP) leaves the contents of the configuration item list to the discretion of the developer. (CM scope (ACM_SCP) can be used to identify specific items that must be included in the configuration item list, and hence covered by CM.)

12.2.4 ACM_CAP.1 Version numbers

Dependencies: No dependencies.

12.2.4.1 Objectives

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

12.2.4.2 Developer action elements

12.2.4.2.1 ACM_CAP.1.1D

The developer shall provide a reference for the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.2.4.3 Content and presentation of evidence elements

12.2.4.3.1 ACM_CAP.1.1C

The reference for the TOE shall be unique to each version of the TOE.

12.2.4.3.2 ACM_CAP.1.2C

The TOE shall be labelled with its reference.

12.2.4.4 Evaluator action elements

12.2.4.4.1 ACM_CAP.1.1E

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

12.2.5 ACM_CAP.2 Configuration items

Dependencies: No dependencies.

12.2.5.1 Objectives

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Unique identification of the configuration items leads to a clearer understanding of the composition of the TOE, which in turn helps to determine those items which are subject to the evaluation requirements for the TOE.

12.2.5.2 Developer action elements

12.2.5.2.1 ACM_CAP.2.1D

The developer shall provide a reference for the TOE.

12.2.5.2.2 ACM_CAP.2.2D

The developer shall use a CM system.

12.2.5.2.3 ACM_CAP.2.3D

The developer shall provide CM documentation.

12.2.5.3 Content and presentation of evidence elements

12.2.5.3.1 ACM_CAP.2.1C

The reference for the TOE shall be unique to each version of the TOE.

12.2.5.3.2 ACM_CAP.2.2C

The TOE shall be labelled with its reference.

12.2.5.3.3 ACM_CAP.2.3C

The CM documentation shall include a configuration list.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.2.5.3.4 ACM_CAP.2.4C

The configuration list shall uniquely identify all configuration items that comprise the TOE.

12.2.5.3.5 ACM_CAP.2.5C

The configuration list shall describe the configuration items that comprise the TOE.

12.2.5.3.6 ACM_CAP.2.6C

The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

12.2.5.3.7 ACM_CAP.2.7C

The CM system shall uniquely identify all configuration items that comprise the TOE.

12.2.5.4 Evaluator action elements

12.2.5.4.1 ACM_CAP.2.1E

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

12.2.6 ACM_CAP.3 Authorisation controls

Dependencies: ALC_DVS.1 Identification of security measures

12.2.6.1 Objectives

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Unique identification of the configuration items leads to a clearer understanding of the composition of the TOE, which in turn helps to determine those items which are subject to the evaluation requirements for the TOE.

Providing controls to ensure that unauthorised modifications are not made to the TOE, and ensuring proper functionality and use of the CM system, helps to maintain the integrity of the TOE.

12.2.6.2 Developer action elements

12.2.6.2.1 ACM_CAP.3.1D

The developer shall provide a reference for the TOE.

12.2.6.2.2 ACM_CAP.3.2D

The developer shall use a CM system.

12.2.6.2.3 ACM_CAP.3.3D

The developer shall provide CM documentation.

12.2.6.3 Content and presentation of evidence elements

12.2.6.3.1 ACM_CAP.3.1C

The reference for the TOE shall be unique to each version of the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.2.6.3.2 ACM_CAP.3.2C

The TOE shall be labelled with its reference.

12.2.6.3.3 ACM_CAP.3.3C

The CM documentation shall include a configuration list **and a CM plan.**

12.2.6.3.4 ACM_CAP.3.4C

The configuration list shall uniquely identify all configuration items that comprise the TOE.

12.2.6.3.5 ACM_CAP.3.5C

The configuration list shall describe the configuration items that comprise the TOE.

12.2.6.3.6 ACM_CAP.3.6C

The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

12.2.6.3.7 ACM_CAP.3.7C

The CM system shall uniquely identify all configuration items that comprise the TOE.

12.2.6.3.8 ACM_CAP.3.8C

The CM plan shall describe how the CM system is used.

12.2.6.3.9 ACM_CAP.3.9C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

12.2.6.3.10 ACM_CAP.3.10C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

12.2.6.3.11 ACM_CAP.3.11C

The CM system shall provide measures such that only authorised changes are made to the configuration items.

12.2.6.4 Evaluator action elements

12.2.6.4.1 ACM_CAP.3.1E

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

12.2.7 ACM_CAP.4 Generation support and acceptance procedures

Dependencies: ALC_DVS.1 Identification of security measures

12.2.7.1 Objectives

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

Unique identification of the configuration items leads to a clearer understanding of the composition of the TOE, which in turn helps to determine those items which are subject to the evaluation requirements for the TOE.

Providing controls to ensure that unauthorised modifications are not made to the TOE, and ensuring proper functionality and use of the CM system, helps to maintain the integrity of the TOE.

The purpose of acceptance procedures is to confirm that any creation or modification of configuration items is authorised.

12.2.7.2 Developer action elements

12.2.7.2.1 ACM_CAP.4.1D

The developer shall provide a reference for the TOE.

12.2.7.2.2 ACM_CAP.4.2D

The developer shall use a CM system.

12.2.7.2.3 ACM_CAP.4.3D

The developer shall provide CM documentation.

12.2.7.3 Content and presentation of evidence elements

12.2.7.3.1 ACM_CAP.4.1C

The reference for the TOE shall be unique to each version of the TOE.

12.2.7.3.2 ACM_CAP.4.2C

The TOE shall be labelled with its reference.

12.2.7.3.3 ACM_CAP.4.3C

The CM documentation shall include a configuration list, a CM plan, **and an acceptance plan.**

12.2.7.3.4 ACM_CAP.4.4C

The configuration list shall uniquely identify all configuration items that comprise the TOE.

12.2.7.3.5 ACM_CAP.4.5C

The configuration list shall describe the configuration items that comprise the TOE.

12.2.7.3.6 ACM_CAP.4.6C

The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

12.2.7.3.7 ACM_CAP.4.7C

The CM system shall uniquely identify all configuration items that comprise the TOE.

12.2.7.3.8 ACM_CAP.4.8C

The CM plan shall describe how the CM system is used.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.2.7.3.9 ACM_CAP.4.9C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

12.2.7.3.10 ACM_CAP.4.10C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

12.2.7.3.11 ACM_CAP.4.11C

The CM system shall provide measures such that only authorised changes are made to the configuration items.

12.2.7.3.12 ACM_CAP.4.12C

The CM system shall support the generation of the TOE.

12.2.7.3.13 ACM_CAP.4.13C

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

12.2.7.4 Evaluator action elements

12.2.7.4.1 ACM_CAP.4.1E

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

12.2.8 ACM_CAP.5 Advanced support

Dependencies: ALC_DVS.2 Sufficiency of security measures

12.2.8.1 Objectives

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Unique identification of the configuration items leads to a clearer understanding of the composition of the TOE, which in turn helps to determine those items which are subject to the evaluation requirements for the TOE.

Providing controls to ensure that unauthorised modifications are not made to the TOE, and ensuring proper functionality and use of the CM system, helps to maintain the integrity of the TOE.

The purpose of acceptance procedures is to confirm that any creation or modification of configuration items is authorised.

Integration procedures help to ensure that generation of the TOE from a managed set of configuration items is correctly performed in an authorised manner.

Requiring that the CM system be able to identify the master copy of the material used to generate the TOE helps to ensure that the integrity of this material is preserved by the appropriate technical, physical and procedural safeguards.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.2.8.2 Developer action elements

12.2.8.2.1 ACM_CAP.5.1D

The developer shall provide a reference for the TOE.

12.2.8.2.2 ACM_CAP.5.2D

The developer shall use a CM system.

12.2.8.2.3 ACM_CAP.5.3D

The developer shall provide CM documentation.

12.2.8.3 Content and presentation of evidence elements

12.2.8.3.1 ACM_CAP.5.1C

The reference for the TOE shall be unique to each version of the TOE.

12.2.8.3.2 ACM_CAP.5.2C

The TOE shall be labelled with its reference.

12.2.8.3.3 ACM_CAP.5.3C

The CM documentation shall include a configuration list, a CM plan, an acceptance plan, **and integration procedures.**

12.2.8.3.4 ACM_CAP.5.4C

The configuration list shall uniquely identify all configuration items that comprise the TOE.

12.2.8.3.5 ACM_CAP.5.5C

The configuration list shall describe the configuration items that comprise the TOE.

12.2.8.3.6 ACM_CAP.5.6C

The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

12.2.8.3.7 ACM_CAP.5.7C

The CM system shall uniquely identify all configuration items that comprise the TOE.

12.2.8.3.8 ACM_CAP.5.8C

The CM plan shall describe how the CM system is used.

12.2.8.3.9 ACM_CAP.5.9C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

12.2.8.3.10 ACM_CAP.5.10C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.2.8.3.11 ACM_CAP.5.11C

The CM system shall provide measures such that only authorised changes are made to the configuration items.

12.2.8.3.12 ACM_CAP.5.12C

The CM system shall support the generation of the TOE.

12.2.8.3.13 ACM_CAP.5.13C

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

12.2.8.3.14 ACM_CAP.5.14C

The integration procedures shall describe how the CM system is applied in the TOE manufacturing process.

12.2.8.3.15 ACM_CAP.5.15C

The CM system shall require that the person responsible for accepting a configuration item into CM is not the person who developed it.

12.2.8.3.16 ACM_CAP.5.16C

The CM system shall clearly identify the configuration items that comprise the TSF.

12.2.8.3.17 ACM_CAP.5.17C

The CM system shall support the audit of all modifications to the TOE, including the originator, date, and time in the audit trail.

12.2.8.3.18 ACM_CAP.5.18C

The CM system shall be able to identify the master copy of all material used to generate the TOE.

12.2.8.3.19 ACM_CAP.5.19C

The CM documentation shall demonstrate that the use of the CM system, together with the development security measures, allow only authorised changes to be made to the TOE.

12.2.8.3.20 ACM_CAP.5.20C

The CM documentation shall demonstrate that the use of the integration procedures ensures that the generation of the TOE is correctly performed in an authorised manner.

12.2.8.3.21 ACM_CAP.5.21C

The CM documentation shall demonstrate that the CM system is sufficient to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

12.2.8.3.22 ACM_CAP.5.22C

The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.2.8.4 Evaluator action elements

12.2.8.4.1 ACM_CAP.5.1E

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

12.3 CM scope (ACM_SCP)

12.3.1 Objectives

The objective of this family is to require items to be included as configuration items and hence placed under the CM requirements of CM capabilities (ACM_CAP). Applying configuration management to these additional items provides additional assurance that the integrity of TOE is maintained.

12.3.2 Component levelling

The components in this family are levelled on the basis of which of the following are required to be included as configuration items: implementation representation; the evaluation evidence required by the assurance components in the ST; security flaws; and development tools and related information.

12.3.3 Application notes

While CM capabilities (ACM_CAP) mandates a list of configuration items and that each item on this list be under CM, other than the TOE itself, CM capabilities (ACM_CAP) leaves the contents of the configuration item list to the discretion of the developer. CM scope (ACM_SCP) narrows this discretion by identifying items that must be included in the configuration item list, and hence come under the CM requirements of CM capabilities (ACM_CAP).

ACM_SCP.1.1C introduces the requirement that the TOE implementation representation be included in the list of configuration items. The TOE implementation representation refers to all hardware, software, and firmware that comprise the physical TOE. In the case of a software-only TOE, the implementation representation may consist solely of source and object code.

ACM_SCP.1.1C also introduces the requirement that the evaluation evidence required by the other assurance components in the ST be included in the list of configuration items.

ACM_SCP.2.1C introduces the requirement that security flaws be included in the list of configuration items. This requires that information regarding previous security flaws and their resolution be maintained, as well as details regarding current security flaws.

ACM_SCP.3.1C introduces the requirement that development tools and other related information be included in the list of configuration items. Examples of development tools are programming languages and compilers. Information pertaining to TOE generation items (such as compiler options, installation/generation options, and build options) is an example of information relating to development tools.

12.3.4 ACM_SCP.1 TOE CM coverage

Dependencies: ACM_CAP.3 Authorisation controls

12.3.4.1 Objectives

A CM system can control changes only to those items that have been placed under CM (i.e., the configuration items identified in the configuration item list). Placing the TOE implementation and the evaluation evidence required by the other assurance components in the ST under CM provides assurance that they have been modified in a controlled manner with proper authorisations.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.3.4.2 Developer action elements

12.3.4.2.1 ACM_SCP.1.1D

The developer shall provide a list of configuration items for the TOE.

12.3.4.3 Content and presentation of evidence elements

12.3.4.3.1 ACM_SCP.1.1C

The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

12.3.4.4 Evaluator action elements

12.3.4.4.1 ACM_SCP.1.1E

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

12.3.5 ACM_SCP.2 Problem tracking CM coverage

Dependencies: ACM_CAP.3 Authorisation controls

12.3.5.1 Objectives

A CM system can control changes only to those items that have been placed under CM (i.e., the configuration items identified in the configuration item list). Placing the TOE implementation and the evaluation evidence required by the other assurance components in the ST under CM provides assurance that they have been modified in a controlled manner with proper authorisations.

Placing security flaws under CM ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution.

12.3.5.2 Developer action elements

12.3.5.2.1 ACM_SCP.2.1D

The developer shall provide a list of configuration items for the TOE.

12.3.5.3 Content and presentation of evidence elements

12.3.5.3.1 ACM_SCP.2.1C

The list of configuration items shall include the following: implementation representation; **security flaws;** and the evaluation evidence required by the assurance components in the ST.

12.3.5.4 Evaluator action elements

12.3.5.4.1 ACM_SCP.2.1E

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

12.3.6 ACM_SCP.3 Development tools CM coverage

Dependencies: ACM_CAP.3 Authorisation controls

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

12.3.6.1 Objectives

A CM system can control changes only to those items that have been placed under CM (i.e., the configuration items identified in the configuration item list). Placing the TOE implementation and the evaluation evidence required by the other assurance components in the ST under CM provides assurance that they have been modified in a controlled manner with proper authorisations.

Placing security flaws under CM ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution.

Development tools play an important role in ensuring the production of a quality version of the TOE. Therefore, it is important to control modifications to these tools.

12.3.6.2 Developer action elements

12.3.6.2.1 ACM_SCP.3.1D

The developer shall provide a list of configuration items for the TOE.

12.3.6.3 Content and presentation of evidence elements

12.3.6.3.1 ACM_SCP.3.1C

The list of configuration items shall include the following: implementation representation; security flaws; **development tools** and **related information; and** the evaluation evidence required by the assurance components in the ST.

12.3.6.4 Evaluator action elements

12.3.6.4.1 ACM_SCP.3.1E

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

13 Class ADO: Delivery and operation

Delivery and operation provides requirements for correct delivery, installation, generation, and start-up of the TOE.

Figure 9 shows the families within this class, and the hierarchy of components within the families.

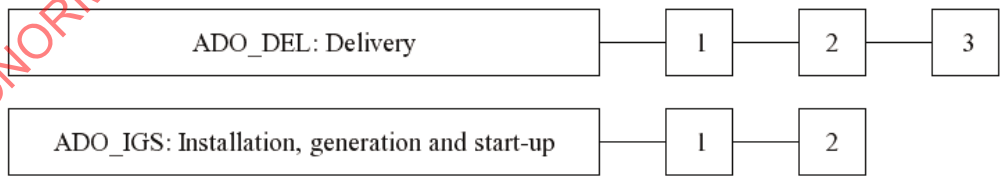


Figure 9 - ADO: Delivery and operation class decomposition

13.1 Delivery (ADO_DEL)

13.1.1 Objectives

The requirements for delivery call for system control and distribution facilities and procedures that detail the measures necessary to provide assurance that the security of the TOE is maintained during distribution of the TOE. For a valid distribution of the TOE, the procedures used for the distribution of the TOE address the threats identified in the PP/ST relating to the security of the TOE during delivery.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

13.1.2 Component levelling

The components in this family are levelled on the basis of increasing requirements on the developer to maintain security of the TOE during delivery.

13.1.3 Application notes

These procedures could consider issues such as:

a) ensuring the TOE received by the consumer corresponds precisely to the TOE Master copy;

b) avoiding/detecting any tampering with the actual version of the TOE;

c) preventing submission of a false version of the TOE;

d) avoiding unwanted knowledge of distribution of the TOE to the consumer;

e) avoiding/detecting the TOE being intercepted during delivery; and

f) avoiding the TOE being delayed or stopped during distribution.

Although the procedures consider protection of the TOE in all aspects (integrity, confidentiality, availability), the technical measures introduced in ADO_DEL.2 Detection of modification and ADO_DEL.3 Prevention of modification are required to address integrity issues only.

13.1.4 ADO_DEL.1 Delivery procedures

Dependencies: No dependencies.

13.1.4.1 Developer action elements

13.1.4.1.1 ADO_DEL.1.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

13.1.4.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

13.1.4.2 Content and presentation of evidence elements

13.1.4.2.1 ADO_DEL.1.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

13.1.4.3 Evaluator action elements

13.1.4.3.1 ADO_DEL.1.1E

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

13.1.5 ADO_DEL.2 Detection of modification

Dependencies: ACM_CAP.3 Authorisation controls

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

13.1.5.1 Developer action elements

13.1.5.1.1 ADO_DEL.2.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

13.1.5.1.2 ADO_DEL.2.2D

The developer shall use the delivery procedures.

13.1.5.2 Content and presentation of evidence elements

13.1.5.2.1 ADO_DEL.2.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

13.1.5.2.2 ADO_DEL.2.2C

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

13.1.5.2.3 ADO_DEL.2.3C

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

13.1.5.3 Evaluator action elements

13.1.5.3.1 ADO_DEL.2.1E

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

13.1.6 ADO_DEL.3 Prevention of modification

Dependencies: ACM_CAP.3 Authorisation controls

13.1.6.1 Developer action elements

13.1.6.1.1 ADO_DEL.3.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

13.1.6.1.2 ADO_DEL.3.2D

The developer shall use the delivery procedures.

13.1.6.2 Content and presentation of evidence elements

13.1.6.2.1 ADO_DEL.3.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

13.1.6.2.2 ADO_DEL.3.2C

The delivery documentation shall describe how the various procedures and technical measures provide for the **prevention** of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

13.1.6.2.3 ADO_DEL.3.3C

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

13.1.6.3 Evaluator action elements

13.1.6.3.1 ADO_DEL.3.1E

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

13.2 Installation, generation and start-up (ADO_IGS)

13.2.1 Objectives

Installation, generation, and start-up procedures are useful for ensuring that the TOE has been installed, generated, and started up in a secure manner as intended by the developer. The requirements for installation, generation and start-up call for a secure transition from the TOE's implementation representation being under configuration control to its initial operation in the user environment.

13.2.2 Component levelling

The components in this family are levelled on the basis of whether the TOE generation options are logged.

13.2.3 Application notes

It is recognised that the application of these requirements will vary depending on aspects such as whether the TOE is an IT product or system, whether it is delivered in an operational state, or whether it has to be brought up at the TOE owner's site, etc. For a given TOE, there will normally be a division of responsibility with respect to installation, generation and start-up between the TOE developer and the owner of the TOE, but there are examples where all activities take place at one site. For example, for a smart card all aspects of installation, generation and start-up may have been performed at the TOE developer's site. On the other hand the TOE might be delivered as an IT system in the form of software, where all aspects of installation, generation and start-up are carried out at the TOE owner's site.

It might also be the case that the TOE is already installed by the time the evaluation starts. In this case it may be inappropriate to demand and analyse installation procedures.

Furthermore, the generation requirements are applicable only to TOEs that provide the ability to generate portions of an operational TOE from its implementation representation.

The installation, generation, and start-up procedures may exist as a separate documents or could be grouped with other administrative guidance. The requirements in this assurance family are presented separately from those in the Administrator guidance (AGD_ADM) family, due to the infrequent, possibly one-time use of the installation, generation and start-up procedures.

13.2.4 ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies: AGD_ADM.1 Administrator guidance

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

13.2.4.1 Developer action elements

13.2.4.1.1 ADO_IGS.1.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

13.2.4.2 Content and presentation of evidence elements

13.2.4.2.1 ADO_IGS.1.1C

The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

13.2.4.3 Evaluator action elements

13.2.4.3.1 ADO_IGS.1.1E

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

13.2.4.3.2 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

13.2.5 ADO_IGS.2 Generation log

Dependencies: AGD_ADM.1 Administrator guidance

13.2.5.1 Developer action elements

13.2.5.1.1 ADO_IGS.2.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

13.2.5.2 Content and presentation of evidence elements

13.2.5.2.1 ADO_IGS.2.1C

The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

13.2.5.2.2 ADO_IGS.2.2C

The installation, generation and start-up documentation shall describe procedures capable of creating a log containing the generation options used to generate the TOE in such a way that it is possible to determine exactly how and when the TOE was generated.

13.2.5.3 Evaluator action elements

13.2.5.3.1 ADO_IGS.2.1E

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

13.2.5.3.2 ADO_IGS.2.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

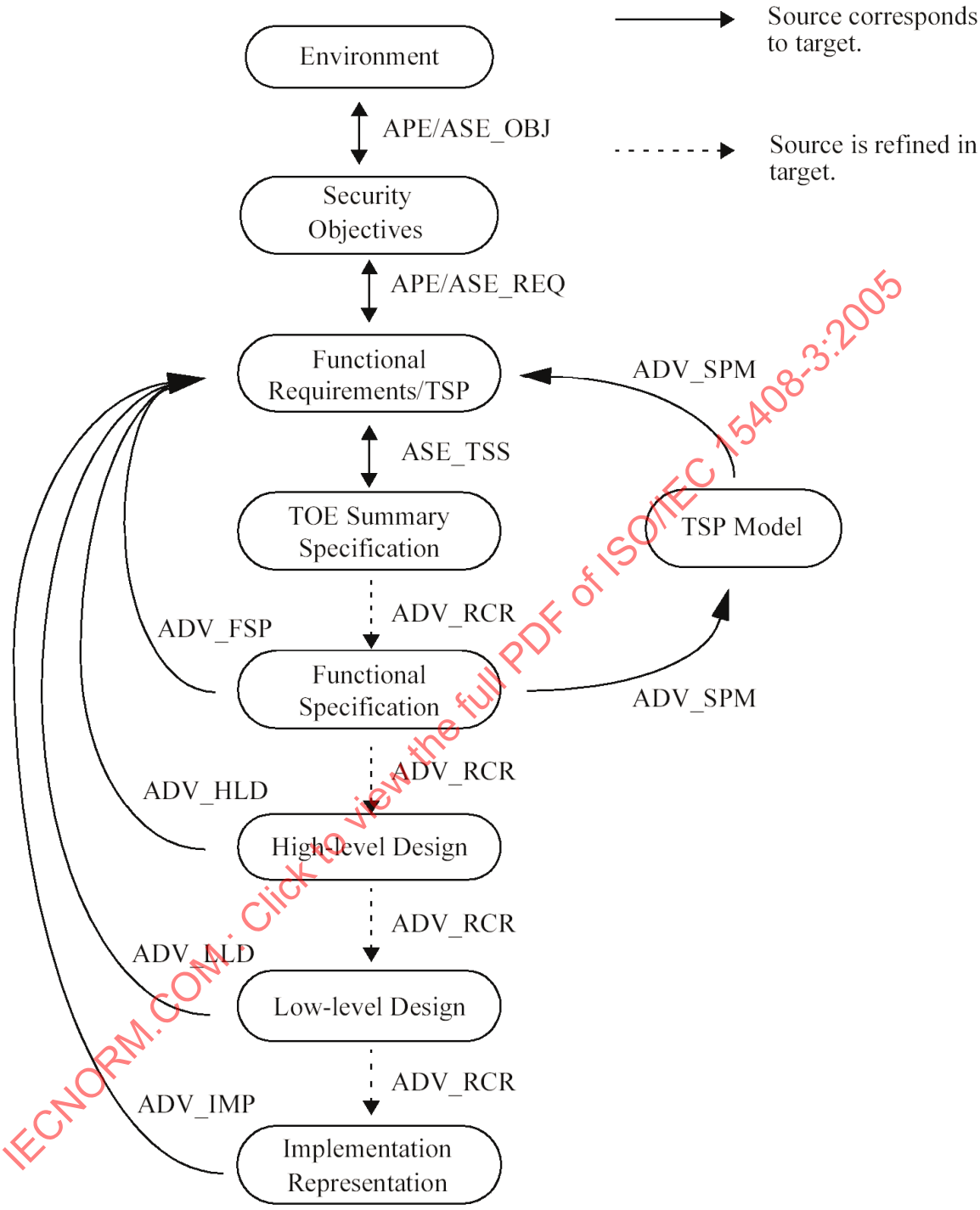
14 Class ADV: Development

The development class encompasses four families of requirements for representing the TSF at various levels of abstraction from the functional interface to the implementation representation. The development class also includes a family of requirements for a correspondence mapping between the various TSF representations, ultimately requiring a demonstration of correspondence from the least abstract representation through all intervening representations to the TOE summary specification provided in the ST. In addition, there is a family of requirements for a TSP model, and for correspondence mappings between the TSP, the TSP model, and the functional specification. Finally, there is a family of requirements on the internal structure of the TSF, which covers aspects such as modularity, layering, and minimisation of complexity.

The paradigm evident for these families is one of a functional specification of the TSF, decomposing the TSF into subsystems, decomposing the subsystems into modules, showing the implementation of the modules, and demonstration of correspondence between all decompositions that are provided as evidence. The requirements for the various TSF representations are separated into different families, however, to allow the PP/ST author to specify which subset of the TSF representations are required.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved



IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

Figure 10 - Relationships between TOE representations and requirements

Figure 10 indicates the relationships between the various TSF representations and the objectives and requirements that they are intended to address. As the figure indicates, the APE and ASE classes define the requirements for the correspondence between the functional requirements and the security objectives as well as between the security objectives and the TOE's anticipated environment. Class ASE also defines requirements for the correspondence between both the security objectives and functional requirements and the TOE summary specification.

© ISO/IEC 2005 - All rights reserved

The requirements for all other correspondence shown in Figure 10 are defined in the ADV: Development class. The Security policy modeling (ADV_SPM) family defines the requirements for correspondence between the TSP and the TSP model, and between the TSP model and the functional specification. The Representation correspondence (ADV_RCR) family defines the requirements for correspondence between all available TSF representations from the TOE summary specification through the implementation representation. Finally, each assurance family specific to a TSF representation (i.e. Functional specification (ADV_FSP), High-level design (ADV_HLD), Low-level design (ADV_LLD) and Implementation representation (ADV_IMP)) defines requirements relating that TSF representation to the functional requirements, the combination of which helps to ensure that the TOE security functional requirements have been addressed. The traceability analysis is always to be performed from the highest-level TSF representation down through each of the TSF representations that are provided. ISO/IEC 15408 captures this traceability requirement via dependencies on the Representation correspondence (ADV_RCR) family. The TSF internals (ADV_INT) family is not represented in this figure, as it is related to the internal structure of the TSF, and is only indirectly related to the process of refinement of the TSF representations.

The TOE security policy (TSP) is the set of rules that regulate how resources are managed, protected and distributed within a TOE, expressed by the TOE security functional requirements. The developer is not explicitly required to provide a TSP, as the TSP is expressed by the TOE security functional requirements, through a combination of security function policies (SFPs) and the other individual requirement elements.

The TOE security functions (TSF) are all the parts of the TOE that have to be relied upon for enforcement of the TSP. The TSF includes both functions that directly enforce the TSP, and also those functions that, while not directly enforcing the TSP, contribute to the enforcement of the TSP in a more indirect manner.

Although the requirements within the TOE summary specification (ASE_TSS) family and within several families of this class call for several different TSF representations, it is not absolutely necessary for each and every TSF representation to be in a separate document. Indeed, it may be the case that a single document meets the documentation requirements for more than one TSF representation, since it is the information about each of these TSF representations that is required, rather than the resulting document structure. In cases where multiple TSF representations are combined within a single document, the developer should indicate which documents meet which requirements.

Three types of specification style are mandated by this class: informal, semiformal and formal. The functional specification, high-level design, low-level design and TSP models will be written using one or more of these specification styles. Ambiguity in these specifications is reduced by using an increased level of formality.

An informal specification is written as prose in natural language. Natural language is used here as meaning communication in any commonly spoken tongue (e.g. Dutch, English, French, German). An informal specification is not subject to any notational or special restrictions other than those required as ordinary conventions for that language (e.g. grammar and syntax). While no notational restrictions apply, the informal specification is also required to provide defined meanings for terms that are used in a context other than that accepted by normal usage.

A semiformal specification is written in a restricted syntax language and is typically accompanied by supporting explanatory (informal) prose. The restricted syntax language may be a natural language with restricted sentence structure and keywords with special meanings, or it may be diagrammatic (e.g. data-flow diagrams, state transition diagrams, entity-relationship diagrams, data structure diagrams, and process or program structure diagrams). Whether based on diagrams or natural language, a set of conventions must be supplied to define the restrictions placed on the syntax.

A formal specification is written in a notation based upon well-established mathematical concepts, and is typically accompanied by supporting explanatory (informal) prose. These mathematical concepts are used to define the syntax and semantics of the notation and the proof rules that support logical reasoning. The syntactic and semantic rules supporting a formal notation should define how to recognise constructs unambiguously and determine their meaning. There needs to be evidence that it is impossible to derive contradictions, and all rules supporting the notation need to be defined or referenced.

Significant assurance can be gained by ensuring that the TSF can be traced through each of its representations, and by ensuring that the TSP model corresponds to the functional specification. The Representation correspondence (ADV_RCR) family contains requirements for correspondence mappings

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

between the various TSF representations, and the Security policy modeling (ADV_SPM) family contains requirements for a correspondence mapping between the TSP model and the functional specification. A correspondence can take the form of an informal demonstration, a semiformal demonstration, or a formal proof.

When an informal demonstration of correspondence is required, this means that only a basic correspondence is required. Correspondence methods include, for example, the use of a two-dimensional table with entries denoting correspondence, or the use of appropriate notation of design diagrams. Pointers and references to other documents may also be used.

A semiformal demonstration of correspondence requires a structured approach at the analysis of the correspondence. This approach should lessen ambiguity that could exist in an informal correspondence by limiting the interpretation of the terms included in the correspondence. Pointers and references to other documents may be used.

A formal proof of correspondence requires that well-established mathematical concepts be used to define the syntax and semantics of the formal notation and the proof rules that support logical reasoning. The security properties need to be expressible in the formal specification language, and these security properties need to be shown to be satisfied by the formal specification. Pointers and references to other documents may also be used.

The Representation correspondence (ADV_RCR).*.1C elements require that the developer provide evidence, for each adjacent pair of TSF representations, that all relevant security functionality of the more abstract TSF representation is refined in the less abstract TSF representation. The Functional specification (ADV_FSP).*.2E, High-level design (ADV_HLD).*.2E, Low-level design (ADV_LLD).*.2E and Implementation representation (ADV_IMP).*.2E elements each require the evaluator to determine that the TSF represented by that family of requirements is an accurate and complete instantiation of the TOE security functional requirements. In order to determine that a TSF representation is an accurate and complete instantiation of the TOE security functional requirements, it is intended that the evaluator use the evidence provided by the developer in Representation correspondence (ADV_RCR).*.1C as an input to this determination. By establishing a correspondence between the TOE security functional requirements and each of successive TSF representations down the chain, this step-wise process will ultimately provide more assurance that the least abstract TSF representation corresponds to the TOE security functional requirements, which is the ultimate goal of this class. If the evaluator makes no correspondence determinations back to the TOE security functional requirements for intermediate TSF representations, then trying to determine the correspondence from the least abstract TSF representation back to the TOE security functional requirements may represent too large a step to be accurately performed. Finally, depending on the set of TSF representations that are required, it is quite possible that the low-level design, high-level design, or even the functional specification might be the least abstract TSF representation that is provided.

Figure 11 shows the families within this class, and the hierarchy of components within the families.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

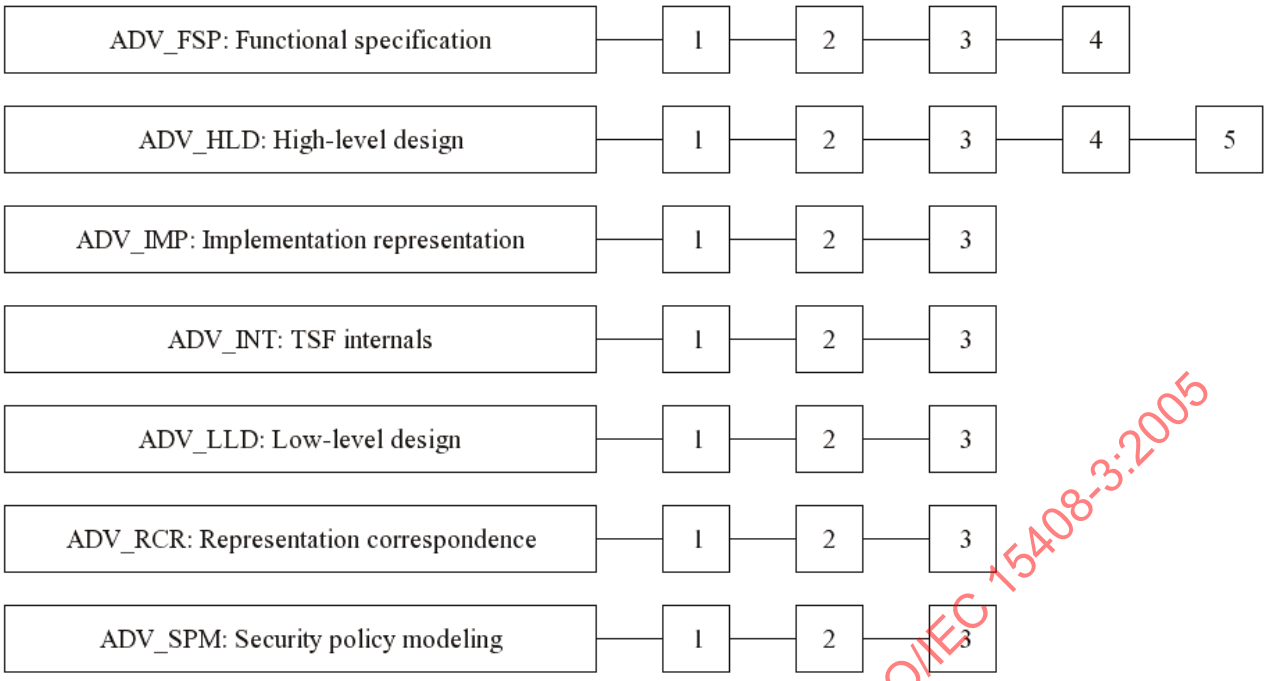


Figure 11 - ADV: Development class decomposition

14.1 Functional specification (ADV_FSP)

14.1.1 Objectives

The functional specification is a high-level description of the user-visible interface and behaviour of the TSF. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all the TOE security functional requirements are addressed.

14.1.2 Component levelling

The components in this family are levelled on the basis of the degree of formalism required of the functional specification, and the degree of detail provided for the external interfaces to the TSF.

14.1.3 Application notes

The Functional specification (ADV_FSP).*.2E elements within this family define a requirement that the evaluator determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the functional specification, in addition to the pairwise correspondences required by the Representation correspondence (ADV_RCR) family. It is expected that the evaluator will use the evidence provided in Representation correspondence (ADV_RCR) as an input to making this determination, and the requirement for completeness is intended to be relative to the level of abstraction of the functional specification.

For ADV_FSP.1.3C, it is intended that sufficient information is provided in the functional specification to understand how the TOE security functional requirements have been addressed, and to enable the specification of tests which reflect the TOE security functional requirements in the ST. It is not necessarily the case that such testing will cover all possible return values and error messages which could be generated at the interface, but the information provided should make clear the results of using an interface in the case of success and the most common instances of failure.

ADV_FSP.2.3C introduces a requirement for a complete presentation of the functional interface. This will provide the necessary detail for supporting both thorough testing of the TOE and the assessment of vulnerabilities.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

In the context of the level of formality of the functional specification, informal, semiformal and formal are considered to be hierarchical in nature. Thus, ADV_FSP.1.1C and ADV_FSP.2.1C may also be met with either a semiformal or formal functional specification, provided that it is supported by informal, explanatory text where appropriate. In addition, ADV_FSP.3.1C may also be met with a formal functional specification.

14.1.4 ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1 Informal correspondence demonstration

14.1.4.1 Developer action elements

14.1.4.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

14.1.4.2 Content and presentation of evidence elements

14.1.4.2.1 ADV_FSP.1.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

14.1.4.2.2 ADV_FSP.1.2C

The functional specification shall be internally consistent.

14.1.4.2.3 ADV_FSP.1.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

14.1.4.2.4 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

14.1.4.3 Evaluator action elements

14.1.4.3.1 ADV_FSP.1.1E

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

14.1.4.3.2 ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

14.1.5 ADV_FSP.2 Fully defined external interfaces

Dependencies: ADV_RCR.1 Informal correspondence demonstration

14.1.5.1 Developer action elements

14.1.5.1.1 ADV_FSP.2.1D

The developer shall provide a functional specification.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.1.5.2 Content and presentation of evidence elements

14.1.5.2.1 ADV_FSP.2.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

14.1.5.2.2 ADV_FSP.2.2C

The functional specification shall be internally consistent.

14.1.5.2.3 ADV_FSP.2.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing **complete** details of **all** effects, exceptions and error messages.

14.1.5.2.4 ADV_FSP.2.4C

The functional specification shall completely represent the TSF.

14.1.5.2.5 ADV_FSP.2.5C

The functional specification shall include rationale that the TSF is completely represented.

14.1.5.3 Evaluator action elements

14.1.5.3.1 ADV_FSP.2.1E

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

14.1.5.3.2 ADV_FSP.2.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

14.1.6 ADV_FSP.3 Semiformal functional specification

Dependencies: ADV_RCR.1 Informal correspondence demonstration

14.1.6.1 Developer action elements

14.1.6.1.1 ADV_FSP.3.1D

The developer shall provide a functional specification.

14.1.6.2 Content and presentation of evidence elements

14.1.6.2.1 ADV_FSP.3.1C

The functional specification shall describe the TSF and its external interfaces using **a semiformal style, supported by** informal, **explanatory text where appropriate.**

14.1.6.2.2 ADV_FSP.3.2C

The functional specification shall be internally consistent.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.1.6.2.3 ADV_FSP.3.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

14.1.6.2.4 ADV_FSP.3.4C

The functional specification shall completely represent the TSF.

14.1.6.2.5 ADV_FSP.3.5C

The functional specification shall include rationale that the TSF is completely represented.

14.1.6.3 Evaluator action elements

14.1.6.3.1 ADV_FSP.3.1E

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

14.1.6.3.2 ADV_FSP.3.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

14.1.7 ADV_FSP.4 Formal functional specification

Dependencies: ADV_RCR.1 Informal correspondence demonstration

14.1.7.1 Developer action elements

14.1.7.1.1 ADV_FSP.4.1D

The developer shall provide a functional specification.

14.1.7.2 Content and presentation of evidence elements

14.1.7.2.1 ADV_FSP.4.1C

The functional specification shall describe the TSF and its external interfaces using a **formal** style, supported by informal, explanatory text where appropriate.

14.1.7.2.2 ADV_FSP.4.2C

The functional specification shall be internally consistent.

14.1.7.2.3 ADV_FSP.4.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

14.1.7.2.4 ADV_FSP.4.4C

The functional specification shall completely represent the TSF.

14.1.7.2.5 ADV_FSP.4.5C

The functional specification shall include rationale that the TSF is completely represented.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.1.7.3 Evaluator action elements

14.1.7.3.1 ADV_FSP.4.1E

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

14.1.7.3.2 ADV_FSP.4.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

14.2 High-level design (ADV_HLD)

14.2.1 Objectives

The high-level design of a TOE provides a description of the TSF in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide. The high-level design requirements are intended to provide assurance that the TOE provides an architecture appropriate to implement the TOE security functional requirements.

The high-level design refines the functional specification into subsystems. For each subsystem of the TSF, the high-level design describes its purpose and function, and identifies the security functions contained in the subsystem. The interrelationships of all subsystems are also defined in the high-level design. These interrelationships will be represented as external interfaces for data flow, control flow, etc., as appropriate.

14.2.2 Component levelling

The components in this family are levelled on the basis of the degree of formalism required of the high-level design, and on the degree of detail required for the interface specifications.

14.2.3 Application notes

The developer is expected to describe the design of the TSF in terms of subsystems. The term “subsystem” is used here to express the idea of decomposing the TSF into a relatively small number of parts. While the developer is not required to actually have “subsystems”, the developer is expected to represent a similar level of decomposition. For example, a design may be similarly decomposed using “layers”, “domains”, or “servers”.

The term “security functionality” is used to represent the set of operations that a subsystem performs in contribution to security functions implemented by the TOE. This distinction is made because design constructs, such as subsystems and modules, do not necessarily relate to specific security functions. While a given subsystem may correspond directly to a security function, or even multiple security functions, it is also possible that many subsystems must be combined to implement a single security function.

The term “TSP-enforcing subsystem” refers to a subsystem that contributes to the enforcement of the TSP, either directly or indirectly.

The High-level design (ADV_HLD).*.2E elements within this family define a requirement that the evaluator determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the high-level design, in addition to the pairwise correspondences required by the Representation correspondence (ADV_RCR) family. It is expected that the evaluator will use the evidence provided in Representation correspondence (ADV_RCR) as an input to making this determination, and the requirement for completeness is intended to be relative to the level of abstraction of the high-level design.

ADV_HLD.3.8C introduces a requirement for a complete presentation for the interfaces to the subsystems. This will provide the necessary detail for supporting both thorough testing of the TOE (using components from Depth (ATE_DPT)), and the assessment of vulnerabilities.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

In the context of the level of formality of the high-level design, informal, semiformal and formal are considered to be hierarchical in nature. Thus, ADV_HLD.1.1C and ADV_HLD.2.1C may also be met with either a semiformal or formal high-level design, and ADV_HLD.3.1C and ADV_HLD.4.1C may also be met with a formal high-level design.

In High-level design (ADV_HLD).*.5C the phrase “underlying hardware, firmware and/or software” concerns the virtual machine on which the TOE runs (if any), rather than mechanisms contained within the TOE (which are covered elsewhere in the component). As such it is a requirement on information about the IT environment.

14.2.4 ADV_HLD.1 Descriptive high-level design

Dependencies: ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

14.2.4.1 Developer action elements

14.2.4.1.1 ADV_HLD.1.1D

The developer shall provide the high-level design of the TSF.

14.2.4.2 Content and presentation of evidence elements

14.2.4.2.1 ADV_HLD.1.1C

The presentation of the high-level design shall be informal.

14.2.4.2.2 ADV_HLD.1.2C

The high-level design shall be internally consistent.

14.2.4.2.3 ADV_HLD.1.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

14.2.4.2.4 ADV_HLD.1.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

14.2.4.2.5 ADV_HLD.1.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

14.2.4.2.6 ADV_HLD.1.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

14.2.4.2.7 ADV_HLD.1.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.2.4.3 Evaluator action elements

14.2.4.3.1 ADV_HLD.1.1E

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

14.2.4.3.2 ADV_HLD.1.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

14.2.5 ADV_HLD.2 Security enforcing high-level design

Dependencies: ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

14.2.5.1 Developer action elements

14.2.5.1.1 ADV_HLD.2.1D

The developer shall provide the high-level design of the TSF.

14.2.5.2 Content and presentation of evidence elements

14.2.5.2.1 ADV_HLD.2.1C

The presentation of the high-level design shall be informal.

14.2.5.2.2 ADV_HLD.2.2C

The high-level design shall be internally consistent.

14.2.5.2.3 ADV_HLD.2.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

14.2.5.2.4 ADV_HLD.2.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

14.2.5.2.5 ADV_HLD.2.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

14.2.5.2.6 ADV_HLD.2.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

14.2.5.2.7 ADV_HLD.2.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.2.5.2.8 ADV_HLD.2.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

14.2.5.2.9 ADV_HLD.2.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

14.2.5.3 Evaluator action elements

14.2.5.3.1 ADV_HLD.2.1E

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

14.2.5.3.2 ADV_HLD.2.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

14.2.6 ADV_HLD.3 Semiformal high-level design

Dependencies: ADV_FSP.3 Semiformal functional specification

ADV_RCR.2 Semiformal correspondence demonstration

14.2.6.1 Developer action elements

14.2.6.1.1 ADV_HLD.3.1D

The developer shall provide the high-level design of the TSF.

14.2.6.2 Content and presentation of evidence elements

14.2.6.2.1 ADV_HLD.3.1C

The presentation of the high-level design shall be **semiformal.**

14.2.6.2.2 ADV_HLD.3.2C

The high-level design shall be internally consistent.

14.2.6.2.3 ADV_HLD.3.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

14.2.6.2.4 ADV_HLD.3.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

14.2.6.2.5 ADV_HLD.3.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.2.6.2.6 ADV_HLD.3.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

14.2.6.2.7 ADV_HLD.3.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

14.2.6.2.8 ADV_HLD.3.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing **complete** details of **all** effects, exceptions and error messages.

14.2.6.2.9 ADV_HLD.3.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

14.2.6.3 Evaluator action elements

14.2.6.3.1 ADV_HLD.3.1E

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

14.2.6.3.2 ADV_HLD.3.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

14.2.7 ADV_HLD.4 Semiformal high-level explanation

Dependencies: ADV_FSP.3 Semiformal functional specification

ADV_RCR.2 Semiformal correspondence demonstration

14.2.7.1 Developer action elements

14.2.7.1.1 ADV_HLD.4.1D

The developer shall provide the high-level design of the TSF.

14.2.7.2 Content and presentation of evidence elements

14.2.7.2.1 ADV_HLD.4.1C

The presentation of the high-level design shall be semiformal.

14.2.7.2.2 ADV_HLD.4.2C

The high-level design shall be internally consistent.

14.2.7.2.3 ADV_HLD.4.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

14.2.7.2.4 ADV_HLD.4.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.2.7.2.5 ADV_HLD.4.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

14.2.7.2.6 ADV_HLD.4.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

14.2.7.2.7 ADV_HLD.4.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

14.2.7.2.8 ADV_HLD.4.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing complete details of all effects, exceptions and error messages.

14.2.7.2.9 ADV_HLD.4.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

14.2.7.2.10 ADV_HLD.4.10C

The high-level design shall justify that the identified means of achieving separation, including any protection mechanisms, are sufficient to ensure a clear and effective separation of TSP-enforcing from non-TSP-enforcing functions.

14.2.7.2.11 ADV_HLD.4.11C

The high-level design shall justify that the TSF mechanisms are sufficient to implement the security functions identified in the high-level design.

14.2.7.3 Evaluator action elements

14.2.7.3.1 ADV_HLD.4.1E

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

14.2.7.3.2 ADV_HLD.4.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

14.2.8 ADV_HLD.5 Formal high-level design

Dependencies: ADV_FSP.4 Formal functional specification

ADV_RCR.3 Formal correspondence demonstration

14.2.8.1 Developer action elements

14.2.8.1.1 ADV_HLD.5.1D

The developer shall provide the high-level design of the TSF.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.2.8.2 Content and presentation of evidence elements

14.2.8.2.1 ADV_HLD.5.1C

The presentation of the high-level design shall be **formal.**

14.2.8.2.2 ADV_HLD.5.2C

The high-level design shall be internally consistent.

14.2.8.2.3 ADV_HLD.5.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

14.2.8.2.4 ADV_HLD.5.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

14.2.8.2.5 ADV_HLD.5.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

14.2.8.2.6 ADV_HLD.5.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

14.2.8.2.7 ADV_HLD.5.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

14.2.8.2.8 ADV_HLD.5.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing complete details of all effects, exceptions and error messages.

14.2.8.2.9 ADV_HLD.5.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

14.2.8.2.10 ADV_HLD.5.10C

The high-level design shall justify that the identified means of achieving separation, including any protection mechanisms, are sufficient to ensure a clear and effective separation of TSP-enforcing from non-TSP-enforcing functions.

14.2.8.2.11 ADV_HLD.5.11C

The high-level design shall justify that the TSF mechanisms are sufficient to implement the security functions identified in the high-level design.

14.2.8.3 Evaluator action elements

14.2.8.3.1 ADV_HLD.5.1E

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.2.8.3.2 ADV_HLD.5.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

14.3 Implementation representation (ADV_IMP)

14.3.1 Objectives

The description of the implementation representation in the form of source code, firmware, hardware drawings, etc. captures the detailed internal workings of the TSF in support of analysis.

14.3.2 Component levelling

The components in this family are levelled on the basis of the completeness and structure of the implementation representation provided.

14.3.3 Application notes

The implementation representation is used to express the notion of the least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement. Source code that is then compiled or a hardware drawing that is used to build the actual hardware are examples of parts of an implementation representation.

It is possible that evaluators may use the implementation representation to directly support other evaluation activities (e.g. vulnerability analysis, test coverage analysis, or identification of additional evaluator tests). It is expected that PP/ST authors will select a component that requires that the implementation is complete and comprehensive enough to address the needs of all other requirements included in the PP/ST.

14.3.4 ADV_IMP.1 Subset of the implementation of the TSF

Dependencies: ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1 Well-defined development tools

14.3.4.1 Application notes

ADV_IMP.1.1D requires that the developer provide the implementation representation for a subset of the TSF. The intention is that access to at least a portion of the TSF will provide the evaluator with an opportunity to examine the implementation representation for those portions of the TOE where such an examination can add significantly to the understanding of, and assurance in, the mechanisms employed. Provision of a sample of the implementation representation will also allow the evaluator to sample the traceability evidence to gain assurance in the approach taken for refinement, and to assess the presentation of the implementation representation itself.

ADV_IMP.1.2E element defines a requirement that the evaluator determine that the least abstract TSF representation is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the least abstract TSF representation, in addition to the pairwise correspondences required by the Representation correspondence (ADV_RCR) family. It is expected that the evaluator will use the evidence provided in Representation correspondence (ADV_RCR) as an input to making this determination. The least abstract TSF representation for this component is an aggregate of the implementation representation that is provided and that portion of the low-level design for which no corresponding implementation representation is provided.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.3.4.2 Developer action elements

14.3.4.2.1 ADV_IMP.1.1D

The developer shall provide the implementation representation for a selected subset of the TSF.

14.3.4.3 Content and presentation of evidence elements

14.3.4.3.1 ADV_IMP.1.1C

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

14.3.4.3.2 ADV_IMP.1.2C

The implementation representation shall be internally consistent.

14.3.4.4 Evaluator action elements

14.3.4.4.1 ADV_IMP.1.1E

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

14.3.4.4.2 ADV_IMP.1.2E

The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

14.3.5 ADV_IMP.2 Implementation of the TSF

Dependencies: ADV_LLD.1 Descriptive low-level design

ALC_TAT.1 Well-defined development tools

14.3.5.1 Application notes

The ADV_IMP.2.2E element defines a requirement that the evaluator determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the implementation representation, in addition to the pairwise correspondences required by the Representation correspondence (ADV_RCR) family. It is expected that the evaluator will use the evidence provided in Representation correspondence (ADV_RCR) as an input to making this determination.

14.3.5.2 Developer action elements

14.3.5.2.1 ADV_IMP.2.1D

The developer shall provide the implementation representation for the **entire** TSF.

14.3.5.3 Content and presentation of evidence elements

14.3.5.3.1 ADV_IMP.2.1C

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.3.5.3.2 ADV_IMP.2.2C

The implementation representation shall be internally consistent.

14.3.5.3.3 ADV_IMP.2.3C

The implementation representation shall describe the relationships between all portions of the implementation.

14.3.5.4 Evaluator action elements

14.3.5.4.1 ADV_IMP.2.1E

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

14.3.5.4.2 ADV_IMP.2.2E

The evaluator shall determine that the **implementation** representation is an accurate and complete instantiation of the TOE security functional requirements.

14.3.6 ADV_IMP.3 Structured implementation of the TSF

Dependencies: ADV_INT.1 Modularity

ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1 Well-defined development tools

14.3.6.1 Application notes

The ADV_IMP.3.2E element defines a requirement that the evaluator determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the implementation representation, in addition to the pairwise correspondences required by the Representation correspondence (ADV_RCR) family. It is expected that the evaluator will use the evidence provided in Representation correspondence (ADV_RCR) as an input to making this determination.

14.3.6.2 Developer action elements

14.3.6.2.1 ADV_IMP.3.1D

The developer shall provide the implementation representation for the entire TSF.

14.3.6.3 Content and presentation of evidence elements

14.3.6.3.1 ADV_IMP.3.1C

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

14.3.6.3.2 ADV_IMP.3.2C

The implementation representation shall be internally consistent.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.3.6.3.3 ADV_IMP.3.3C

The implementation representation shall describe the relationships between all portions of the implementation.

14.3.6.3.4 ADV_IMP.3.4C

The implementation representation shall be structured into small and comprehensible subclauses.

14.3.6.4 Evaluator action elements

14.3.6.4.1 ADV_IMP.3.1E

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

14.3.6.4.2 ADV_IMP.3.2E

The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

14.4 TSF internals (ADV_INT)

14.4.1 Objectives

This family addresses the internal structure of the TSF. Requirements are presented for modularity, layering (to separate levels of abstraction and minimise circular dependencies), minimisation of the complexity of policy enforcement mechanisms, and the minimisation of the amount of non-TSP-enforcing functionality within the TSF -- thus resulting in a TSF that is simple enough to be analysed.

Modular design reduces the interdependence between elements of the TSF and thus reduces the risk that a change or error in one module will have effects throughout the TOE. Thus, a modular design provides the basis for determining the scope of interaction with other elements of the TSF, provides for increased assurance that unexpected effects do not occur, and also provides the basis for designing and evaluating test suites.

The use of layering and of simpler designs for the TSP-enforcing functionality reduces the complexity of the TSF. This in turn enables a better understanding of the TSF, providing more assurance that the TOE security functional requirements are accurately and completely instantiated in the implementation.

Minimising the amount of functionality in the TSF that does not enforce the TSP, reduces the possibility of flaws in the TSF. In combination with modularity and layering, it allows the evaluator to focus only on that functionality which is necessary for TSP enforcement.

Design complexity minimisation contributes to the assurance that the code is understood -- the less complex the code in the TSF, the greater the likelihood that the design of the TSF is comprehensible. Design complexity minimisation is a key characteristic of a reference validation mechanism.

14.4.2 Component levelling

The components in this family are levelled on the basis of the amount of structure and minimisation required.

14.4.3 Application notes

The term “portions of the TSF” is used to represent parts of the TSF with a varying granularity based on the available TSF representations. The functional specification allows identification in terms of interfaces, the high-level design allows identification in terms of subsystems, the low-level design allows identification in terms of modules, and the implementation representation allows identification in terms of implementation units.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

The ADV_INT.2.5C and ADV_INT.3.5C elements address minimisation of mutual interactions between layers. Nevertheless, it is still permissible to have mutual interactions between layers, but in such cases the developer is required to demonstrate that these mutual interactions are necessary and cannot reasonably be avoided.

ADV_INT.2.6C introduces a reference monitor concept by requiring the minimisation of complexity of the portions of the TSF that enforce the access control and/or information flow control policies identified in the TSP. ADV_INT.3.6C further develops the reference monitor concept by requiring minimisation of the complexity of the entire TSF.

Several of the elements within the components for this family refer to the architectural description. The architectural description is at a similar level of abstraction to the low-level design, in that it is concerned with the modules of the TSF. Whereas the low-level design describes the design of the modules of the TSF, the purpose of the architectural description is to provide evidence of modularity, layering, and minimisation of complexity of the TSF, as applicable. Both the low-level design and the implementation representation are required to be in compliance with the architectural description, to provide assurance that these TSF representations possess the required modularity, layering, and minimisation of complexity.

14.4.4 ADV_INT.1 Modularity

Dependencies: ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

14.4.4.1 Developer action elements

14.4.4.1.1 ADV_INT.1.1D

The developer shall design and structure the TSF in a modular fashion that avoids unnecessary interactions between the modules of the design.

14.4.4.1.2 ADV_INT.1.2D

The developer shall provide an architectural description.

14.4.4.2 Content and presentation of evidence elements

14.4.4.2.1 ADV_INT.1.1C

The architectural description shall identify the modules of the TSF.

14.4.4.2.2 ADV_INT.1.2C

The architectural description shall describe the purpose, interface, parameters, and effects of each module of the TSF.

14.4.4.2.3 ADV_INT.1.3C

The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

14.4.4.3 Evaluator action elements

14.4.4.3.1 ADV_INT.1.1E

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.4.4.3.2 ADV_INT.1.2E

The evaluator shall determine that both the low-level design and the implementation representation are in compliance with the architectural description.

14.4.5 ADV_INT.2 Reduction of complexity

Dependencies: ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

14.4.5.1 Application notes

This component introduces a reference monitor concept by requiring the minimisation of complexity of the portions of the TSF that enforce the access control and/or information flow control policies identified in the TSP.

14.4.5.2 Developer action elements

14.4.5.2.1 ADV_INT.2.1D

The developer shall design and structure the TSF in a modular fashion that avoids unnecessary interactions between the modules of the design.

14.4.5.2.2 ADV_INT.2.2D

The developer shall provide an architectural description.

14.4.5.2.3 ADV_INT.2.3D

The developer shall design and structure the TSF in a layered fashion that minimises mutual interactions between the layers of the design.

14.4.5.2.4 ADV_INT.2.4D

The developer shall design and structure the TSF in such a way that minimises the complexity of the portions of the TSF that enforce any access control and/or information flow control policies.

14.4.5.3 Content and presentation of evidence elements

14.4.5.3.1 ADV_INT.2.1C

The architectural description shall identify the modules of the TSF **and shall specify which portions of the TSF enforce the access control and/or information flow control policies.**

14.4.5.3.2 ADV_INT.2.2C

The architectural description shall describe the purpose, interface, parameters, and effects of each module of the TSF.

14.4.5.3.3 ADV_INT.2.3C

The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

14.4.5.3.4 ADV_INT.2.4C

The architectural description shall describe the layering architecture.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.4.5.3.5 ADV_INT.2.5C

The architectural description shall show that mutual interactions have been minimised, and justify those that remain.

14.4.5.3.6 ADV_INT.2.6C

The architectural description shall describe how the portions of the TSF that enforce any access control and/or information flow control policies have been structured to minimise complexity.

14.4.5.4 Evaluator action elements

14.4.5.4.1 ADV_INT.2.1E

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

14.4.5.4.2 ADV_INT.2.2E

The evaluator shall determine that both the low-level design and the implementation representation are in compliance with the architectural description.

14.4.6 ADV_INT.3 Minimisation of complexity

Dependencies: ADV_IMP.2 Implementation of the TSF

ADV_LLD.1 Descriptive low-level design

14.4.6.1 Application notes

This component requires that the reference monitor property “simple enough to be analysed” is fully addressed. When this component is combined with the functional requirements FPT_RVM.1 and FPT_SEP.3, the reference monitor concept would be fully realised.

14.4.6.2 Developer action elements

14.4.6.2.1 ADV_INT.3.1D

The developer shall design and structure the TSF in a modular fashion that avoids unnecessary interactions between the modules of the design.

14.4.6.2.2 ADV_INT.3.2D

The developer shall provide an architectural description.

14.4.6.2.3 ADV_INT.3.3D

The developer shall design and structure the TSF in a layered fashion that minimises mutual interactions between the layers of the design.

14.4.6.2.4 ADV_INT.3.4D

The developer shall design and structure the TSF in such a way that minimises the complexity of the **entire** TSF.

14.4.6.2.5 ADV_INT.3.5D

The developer shall design and structure the portions of the TSF that enforce any access control and/or information flow control policies such that they are simple enough to be analysed.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.4.6.2.6 ADV_INT.3.6D

The developer shall ensure that functions whose objectives are not relevant for the TSF are excluded from the TSF modules.

14.4.6.3 Content and presentation of evidence elements

14.4.6.3.1 ADV_INT.3.1C

The architectural description shall identify the modules of the TSF and shall specify which portions of the TSF enforce the access control and/or information flow control policies.

14.4.6.3.2 ADV_INT.3.2C

The architectural description shall describe the purpose, interface, parameters, and effects of each module of the TSF.

14.4.6.3.3 ADV_INT.3.3C

The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

14.4.6.3.4 ADV_INT.3.4C

The architectural description shall describe the layering architecture.

14.4.6.3.5 ADV_INT.3.5C

The architectural description shall show that mutual interactions have been minimised, and justify those that remain.

14.4.6.3.6 ADV_INT.3.6C

The architectural description shall describe how the **entire** TSF **has** been structured to minimise complexity.

14.4.6.3.7 ADV_INT.3.7C

The architectural description shall justify the inclusion of any non-TSP-enforcing modules in the TSF.

14.4.6.4 Evaluator action elements

14.4.6.4.1 ADV_INT.3.1E

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

14.4.6.4.2 ADV_INT.3.2E

The evaluator shall determine that both the low-level design and the implementation representation are in compliance with the architectural description.

14.4.6.4.3 ADV_INT.3.3E

The evaluator shall confirm that the portions of the TSF that enforce any access control and/or information flow control policies are simple enough to be analysed.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.5 Low-level design (ADV_LLD)

14.5.1 Objectives

The low-level design of a TOE provides a description of the internal workings of the TSF in terms of modules and their interrelationships and dependencies. The low-level design provides assurance that the TSF subsystems have been correctly and effectively refined.

For each module of the TSF, the low-level design describes its purpose, function, interfaces, dependencies, and the implementation of any TSP-enforcing functions.

14.5.2 Component levelling

The components in this family are levelled on the basis of the degree of formalism required of the low-level design, and on the degree of detail required for the interface specifications.

14.5.3 Application notes

The term “TSP-enforcing module” refers to any module that must be relied upon for correct enforcement of the TSP.

The term “security functionality” is used to represent the set of operations that a module performs in contribution to security functions implemented by the TOE. This distinction is made because modules do not necessarily relate to specific security functions. While a given module may correspond directly to a security function, or even multiple security functions, it is also possible that many modules must be combined to implement a single security function.

The Low-level design (ADV_LLD).*.6C elements require that the low-level design describe how each TSP-enforcing function is provided. The intent of this requirement is that the low-level design provide a description of how each module is expected to be implemented from a design perspective.

The Low-level design (ADV_LLD).*.2E elements within this family define a requirement that the evaluator determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the low-level design, in addition to the pairwise correspondences required by the Representation correspondence (ADV_RCR) family. It is expected that the evaluator will use the evidence provided in Representation correspondence (ADV_RCR) as an input to making this determination, and the requirement for completeness is intended to be relative to the level of abstraction of the low-level design.

ADV_LLD.2.9C introduces a requirement for a complete presentation for the interfaces to the modules. This will provide the necessary detail for supporting both thorough testing of the TOE (using components from Depth (ATE_DPT)), and the assessment of vulnerabilities.

In the context of the level of formality of the low-level design, informal, semiformal and formal are considered to be hierarchical in nature. Thus, ADV_LLD.1.1C may also be met with either a semiformal or formal low-level design, and ADV_LLD.2.1C may also be met with a formal low-level design.

14.5.4 ADV_LLD.1 Descriptive low-level design

Dependencies: ADV_HLD.2 Security enforcing high-level design

ADV_RCR.1 Informal correspondence demonstration

14.5.4.1 Developer action elements

14.5.4.1.1 ADV_LLD.1.1D

The developer shall provide the low-level design of the TSF.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.5.4.2 Content and presentation of evidence elements

14.5.4.2.1 ADV_LLD.1.1C

The presentation of the low-level design shall be informal.

14.5.4.2.2 ADV_LLD.1.2C

The low-level design shall be internally consistent.

14.5.4.2.3 ADV_LLD.1.3C

The low-level design shall describe the TSF in terms of modules.

14.5.4.2.4 ADV_LLD.1.4C

The low-level design shall describe the purpose of each module.

14.5.4.2.5 ADV_LLD.1.5C

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

14.5.4.2.6 ADV_LLD.1.6C

The low-level design shall describe how each TSP-enforcing function is provided.

14.5.4.2.7 ADV_LLD.1.7C

The low-level design shall identify all interfaces to the modules of the TSF.

14.5.4.2.8 ADV_LLD.1.8C

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

14.5.4.2.9 ADV_LLD.1.9C

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

14.5.4.2.10 ADV_LLD.1.10C

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

14.5.4.3 Evaluator action elements

14.5.4.3.1 ADV_LLD.1.1E

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

14.5.4.3.2 ADV_LLD.1.2E

The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.5.5 ADV_LLD.2 Semiformal low-level design

Dependencies: ADV_HLD.3 Semiformal high-level design

ADV_RCR.2 Semiformal correspondence demonstration

14.5.5.1 Developer action elements

14.5.5.1.1 ADV_LLD.2.1D

The developer shall provide the low-level design of the TSF.

14.5.5.2 Content and presentation of evidence elements

14.5.5.2.1 ADV_LLD.2.1C

The presentation of the low-level design shall be **semiformal.**

14.5.5.2.2 ADV_LLD.2.2C

The low-level design shall be internally consistent.

14.5.5.2.3 ADV_LLD.2.3C

The low-level design shall describe the TSF in terms of modules.

14.5.5.2.4 ADV_LLD.2.4C

The low-level design shall describe the purpose of each module.

14.5.5.2.5 ADV_LLD.2.5C

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

14.5.5.2.6 ADV_LLD.2.6C

The low-level design shall describe how each TSP-enforcing function is provided.

14.5.5.2.7 ADV_LLD.2.7C

The low-level design shall identify all interfaces to the modules of the TSF.

14.5.5.2.8 ADV_LLD.2.8C

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

14.5.5.2.9 ADV_LLD.2.9C

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing **complete** details of **all** effects, exceptions and error messages.

14.5.5.2.10 ADV_LLD.2.10C

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.5.5.3 Evaluator action elements

14.5.5.3.1 ADV_LLD.2.1E

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

14.5.5.3.2 ADV_LLD.2.2E

The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

14.5.6 ADV_LLD.3 Formal low-level design

Dependencies: ADV_HLD.5 Formal high-level design

ADV_RCR.3 Formal correspondence demonstration

14.5.6.1 Developer action elements

14.5.6.1.1 ADV_LLD.3.1D

The developer shall provide the low-level design of the TSF.

14.5.6.2 Content and presentation of evidence elements

14.5.6.2.1 ADV_LLD.3.1C

The presentation of the low-level design shall be **formal.**

14.5.6.2.2 ADV_LLD.3.2C

The low-level design shall be internally consistent.

14.5.6.2.3 ADV_LLD.3.3C

The low-level design shall describe the TSF in terms of modules.

14.5.6.2.4 ADV_LLD.3.4C

The low-level design shall describe the purpose of each module.

14.5.6.2.5 ADV_LLD.3.5C

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

14.5.6.2.6 ADV_LLD.3.6C

The low-level design shall describe how each TSP-enforcing function is provided.

14.5.6.2.7 ADV_LLD.3.7C

The low-level design shall identify all interfaces to the modules of the TSF.

14.5.6.2.8 ADV_LLD.3.8C

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.5.6.2.9 ADV_LLD.3.9C

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing complete details of all effects, exceptions and error messages.

14.5.6.2.10 ADV_LLD.3.10C

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

14.5.6.3 Evaluator action elements

14.5.6.3.1 ADV_LLD.3.1E

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

14.5.6.3.2 ADV_LLD.3.2E

The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

14.6 Representation correspondence (ADV_RCR)

14.6.1 Objectives

The correspondence between the various TSF representations (i.e. TOE summary specification, functional specification, high-level design, low-level design, implementation representation) addresses the correct and complete instantiation of the requirements to the least abstract TSF representation provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.

14.6.2 Component levelling

The components in this family are levelled on the basis of the required level of formality of the correspondence between the various TSF representations.

14.6.3 Application notes

The developer must demonstrate to the evaluator that the most detailed, or least abstract, TSF representation provided is an accurate, consistent, and complete instantiation of the functions expressed as functional requirements in the ST. This is accomplished by showing correspondence between adjacent representations at a commensurate level of rigour.

This family of requirements is not intended to address correspondence relating to the TSP model or the TSP. Rather, as shown in Figure 10, it is intended to address correspondence between various TSF representations (i.e. the TOE summary specification, functional specification, high-level design, low-level design, and implementation representation) that are provided.

The Representation correspondence (ADV_RCR).*.1C Elements refer to “all relevant security functionality” in defining the scope of what must be refined between an adjacent pair of TSF representations. For the refinements between the TOE summary specification and the functional specification, this element requires only that the TOE security functions in the TOE summary specification be refined in the functional specification, and does not require that the functional specification contain any details regarding assurance measures (which are presented in the TOE summary specification). Where the implementation representation is only provided for a subset of the TSF (as in ADV_IMP.1 Subset of the implementation of the TSF), the required refinements between the low-level design and the implementation representation are limited to the security functionality that is presented in the implementation representation. In all other cases, this element requires that all parts of the more abstract TSF representation be refined in the less abstract TSF representation.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

In the context of the level of formality for correspondence between adjacent TSF representations, informal, semiformal and formal are considered to be hierarchical in nature. Thus, ADV_RCR.2.2C and ADV_RCR.3.2C may be met with a formal proof of correspondence, and in the absence of any requirements on its level of formality, a demonstration of correspondence may be informal, semiformal or formal.

14.6.4 ADV_RCR.1 Informal correspondence demonstration

Dependencies: No dependencies.

14.6.4.1 Developer action elements

14.6.4.1.1 ADV_RCR.1.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

14.6.4.2 Content and presentation of evidence elements

14.6.4.2.1 ADV_RCR.1.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

14.6.4.3 Evaluator action elements

14.6.4.3.1 ADV_RCR.1.1E

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

14.6.5 ADV_RCR.2 Semiformal correspondence demonstration

Dependencies: No dependencies.

14.6.5.1 Developer action elements

14.6.5.1.1 ADV_RCR.2.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

14.6.5.2 Content and presentation of evidence elements

14.6.5.2.1 ADV_RCR.2.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

14.6.5.2.2 ADV_RCR.2.2C

For each adjacent pair of provided TSF representations, where portions of both representations are at least semiformally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.6.5.3 Evaluator action elements

14.6.5.3.1 ADV_RCR.2.1E

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

14.6.6 ADV_RCR.3 Formal correspondence demonstration

Dependencies: No dependencies.

14.6.6.1 Application notes

The developer must either demonstrate or prove correspondence, as described in the requirements below, commensurate with the level of rigour of presentation style. For example, correspondence must be proven when corresponding representations are formally specified.

14.6.6.2 Developer action elements

14.6.6.2.1 ADV_RCR.3.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

14.6.6.3 Content and presentation of evidence elements

14.6.6.3.1 ADV_RCR.3.2D

For those corresponding portions of representations that are formally specified, the developer shall prove that correspondence.

14.6.6.3.2 ADV_RCR.3.1C

For each adjacent pair of provided TSF representations, the analysis shall **prove or** demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

14.6.6.3.3 ADV_RCR.3.2C

For each adjacent pair of provided TSF representations, where portions of **one representation** are **semiformally specified and the other** at least semiformally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.

14.6.6.3.4 ADV_RCR.3.3C

For each adjacent pair of provided TSF representations, where portions of both representations are formally specified, the proof of correspondence between those portions of the representations shall be formal.

14.6.6.4 Evaluator action elements

14.6.6.4.1 ADV_RCR.3.1E

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.6.6.4.2 ADV_RCR.3.2E

The evaluator shall determine the accuracy of the proofs of correspondence by selectively verifying the formal analysis.

14.7 Security policy modeling (ADV_SPM)

14.7.1 Objectives

It is the objective of this family to provide additional assurance that the security functions in the functional specification enforce the policies in the TSP. This is accomplished via the development of a security policy model that is based on a subset of the policies of the TSP, and establishing a correspondence between the functional specification, the security policy model, and these policies of the TSP.

14.7.2 Component levelling

The components in this family are levelled on the basis of the degree of formality required of the TSP model, and the degree of formality required of the correspondence between the TSP model and the functional specification.

14.7.3 Application notes

While a TSP may include any policies, TSP models have traditionally represented only subsets of those policies, because modeling certain policies is currently beyond the state of the art. The current state of the art determines the policies that can be modeled, and the PP/ST author should identify specific functions and associated policies that can, and thus are required to be, modeled. At the very least, access control and information flow control policies are required to be modeled (if they are part of the TSP) since they are within the state of the art.

For each of the components within this family, there is a requirement to describe the rules and characteristics of applicable policies of the TSP in the TSP model and to ensure that the TSP model satisfies the corresponding policies of the TSP. The “rules” and “characteristics” of a TSP model are intended to allow flexibility in the type of model that may be developed (e.g. state transition, non-interference). For example, rules may be represented as “properties” (e.g. simple security property) and characteristics may be represented as definitions such as “initial state”, “secure state”, “subjects” and “objects”.

In the context of the level of formality of the TSP model and the correspondence between the TSP model and the functional specification, informal, semiformal and formal are considered to be hierarchical in nature. Thus, ADV_SPM.1.1C may also be met with either a semiformal or formal TSP model, and ADV_SPM.2.1C may also be met with a formal TSP model. Furthermore, ADV_SPM.2.5C and ADV_SPM.3.5C may be met with a formal proof of correspondence. Finally, in the absence of any requirements on its level of formality, a demonstration of correspondence may be informal, semiformal or formal.

14.7.4 ADV_SPM.1 Informal TOE security policy model

Dependencies: ADV_FSP.1 Informal functional specification

14.7.4.1 Developer action elements

14.7.4.1.1 ADV_SPM.1.1D

The developer shall provide a TSP model.

14.7.4.1.2 ADV_SPM.1.2D

The developer shall demonstrate correspondence between the functional specification and the TSP model.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.7.4.2 Content and presentation of evidence elements

14.7.4.2.1 ADV_SPM.1.1C

The TSP model shall be informal.

14.7.4.2.2 ADV_SPM.1.2C

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

14.7.4.2.3 ADV_SPM.1.3C

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

14.7.4.2.4 ADV_SPM.1.4C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

14.7.4.3 Evaluator action elements

14.7.4.3.1 ADV_SPM.1.1E

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

14.7.5 ADV_SPM.2 Semiformal TOE security policy model

Dependencies: ADV_FSP.1 Informal functional specification

14.7.5.1 Developer action elements

14.7.5.1.1 ADV_SPM.2.1D

The developer shall provide a TSP model.

14.7.5.1.2 ADV_SPM.2.2D

The developer shall demonstrate correspondence between the functional specification and the TSP model.

14.7.5.2 Content and presentation of evidence elements

14.7.5.2.1 ADV_SPM.2.1C

The TSP model shall be **semiformal.**

14.7.5.2.2 ADV_SPM.2.2C

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

14.7.5.2.3 ADV_SPM.2.3C

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.7.5.2.4 ADV_SPM.2.4C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

14.7.5.2.5 ADV_SPM.2.5C

Where the functional specification is at least semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.

14.7.5.3 Evaluator action elements

14.7.5.3.1 ADV_SPM.2.1E

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

14.7.6 ADV_SPM.3 Formal TOE security policy model

Dependencies: ADV_FSP.1 Informal functional specification

14.7.6.1 Developer action elements

14.7.6.1.1 ADV_SPM.3.1D

The developer shall provide a TSP model.

14.7.6.1.2 ADV_SPM.3.2D

The developer shall demonstrate **or prove, as appropriate,** correspondence between the functional specification and the TSP model.

14.7.6.2 Content and presentation of evidence elements

14.7.6.2.1 ADV_SPM.3.1C

The TSP model shall be **formal.**

14.7.6.2.2 ADV_SPM.3.2C

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

14.7.6.2.3 ADV_SPM.3.3C

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

14.7.6.2.4 ADV_SPM.3.4C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

14.7.6.2.5 ADV_SPM.3.5C

Where the functional specification is semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

14.7.6.2.6 ADV_SPM.3.6C

Where the functional specification is formal, the proof of correspondence between the TSP model and the functional specification shall be formal.

14.7.6.3 Evaluator action elements

14.7.6.3.1 ADV_SPM.3.1E

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

15 Class AGD: Guidance documents

The guidance documents class provides the requirements for user and administrator guidance documentation. For the secure administration and use of the TOE it is necessary to describe all relevant aspects for the secure application of the TOE. Guidance documentation includes user and administrator guidance and, when included in the assurance package, the specific guidance for users and administrators resulting from the requirements in the ADO: Delivery and operation class and the Flaw remediation (ALC_FLR) family.

Figure 12 shows the families within this class, and the hierarchy of components within the families.

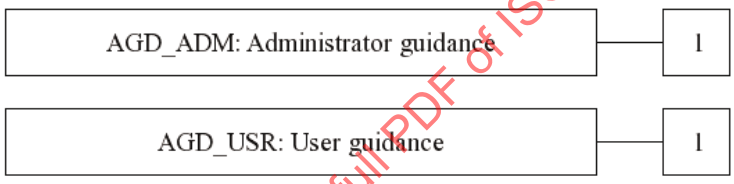


Figure 12 - AGD: Guidance documents class decomposition

15.1 Administrator guidance (AGD_ADM)

15.1.1 Objectives

Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. Because the secure operation of the TOE is dependent upon the correct performance of the TSF, persons responsible for performing these functions are trusted by the TSF. Administrator guidance is intended to help administrators understand the security functions provided by the TOE, including both those functions that require the administrator to perform security-critical actions and those functions that provide security-critical information.

15.1.2 Component levelling

This family contains only one component.

15.1.3 Application notes

The requirements AGD_ADM.1.3C and AGD_ADM.1.7C encompass the aspect that any warnings to the users of a TOE with regard to the TOE security environment and the security objectives described in the PP/ST are appropriately covered in the administrator guidance.

The concept of secure values, as employed in AGD_ADM.1.5C, has relevance where an administrator has control over security parameters. Guidance needs to be provided on secure and insecure settings for such parameters. This concept is related to the use of the component FMT_MSA.2 from ISO/IEC 15408-2.

AGD_ADM.1.6C requires that the administrator guidance describe the appropriate administrator's reactions to all security-relevant events. Although many security-relevant events are the result of performing administrative functions, this need not always be the case (e.g. the audit log fills up, an intrusion is detected). Furthermore, a

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

security-relevant event may happen as a result of a specific chain of administrator functions or, conversely, several security-relevant events may be triggered by one function.

15.1.4 AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1 Informal functional specification

15.1.4.1 Developer action elements

15.1.4.1.1 AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

15.1.4.2 Content and presentation of evidence elements

15.1.4.2.1 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

15.1.4.2.2 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

15.1.4.2.3 AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

15.1.4.2.4 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

15.1.4.2.5 AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

15.1.4.2.6 AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

15.1.4.2.7 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documentation supplied for evaluation.

15.1.4.2.8 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

15.1.4.3 Evaluator action elements

15.1.4.3.1 AGD_ADM.1.1E

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

15.2 User guidance (AGD_USR)

15.2.1 Objectives

User guidance refers to material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE's external interfaces. User guidance describes the security functions provided by the TSF and provides instructions and guidelines, including warnings, for its secure use.

The user guidance provides a basis for assumptions about the use of the TOE and a measure of confidence that non-malicious users, application providers and others exercising the external interfaces of the TOE will understand the secure operation of the TOE and will use it as intended.

15.2.2 Component levelling

This family contains only one component.

15.2.3 Application notes

The requirements AGD_USR.1.3C and AGD_USR.1.5C encompass the aspect that any warnings to the users of a TOE with regard to the TOE security environment and the security objectives described in the PP/ST are appropriately covered in the user guidance.

In many cases it may be appropriate that guidance is provided in separate documents: one for human users, and one for application programmers and/or hard-ware designers using software or hardware interfaces.

15.2.4 AGD_USR.1 User guidance

Dependencies: ADV_FSP.1 Informal functional specification

15.2.4.1 Developer action elements

15.2.4.1.1 AGD_USR.1.1D

The developer shall provide user guidance.

15.2.4.2 Content and presentation of evidence elements

15.2.4.2.1 AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

15.2.4.2.2 AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

15.2.4.2.3 AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

15.2.4.2.4 AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

15.2.4.2.5 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

15.2.4.2.6 AGD_USR.1.6C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

15.2.4.3 Evaluator action elements

15.2.4.3.1 AGD_USR.1.1E

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

16 Class ALC: Life cycle support

Life-cycle support is an aspect of establishing discipline and control in the processes of refinement of the TOE during its development and maintenance. Confidence in the correspondence between the TOE security requirements and the TOE is greater if security analysis and the production of the evidence are done on a regular basis as an integral part of the development and maintenance activities.

Figure 13 shows the families within this class, and the hierarchy of components within the families.

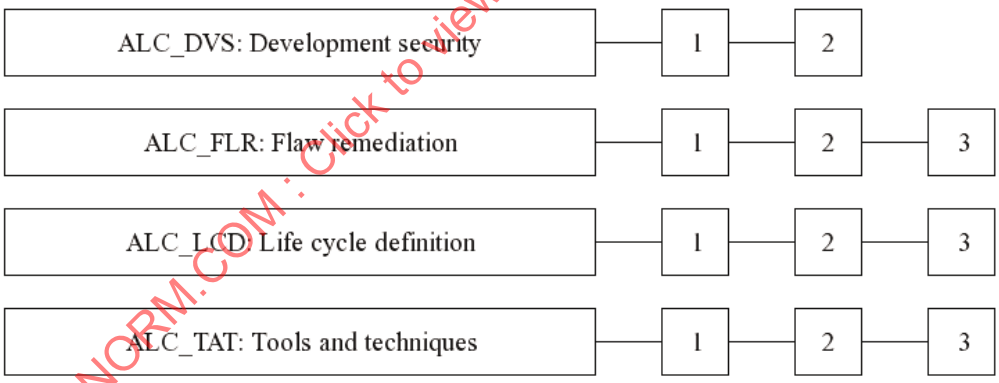


Figure 13 - ALC: Life cycle support class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

16.1 Development security (ALC_DVS)

16.1.1 Objectives

Development security is concerned with physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE. It includes the physical security of the development location and any procedures used to select development staff.

16.1.2 Component levelling

The components in this family are levelled on the basis of whether justification of the sufficiency of the security measures is required.

© ISO/IEC 2005 - All rights reserved

16.1.3 Application notes

This family deals with measures to remove or reduce threats existing at the developer's site. Conversely, threats to be countered at the TOE user's site are normally covered in the security environment subclause of a PP or ST.

The evaluator should determine whether there is a need for visiting the developer's site in order to confirm that the requirements of this family are met.

It is recognised that confidentiality may not always be an issue for the protection of the TOE in its development environment. The use of the word “necessary” allows for the selection of appropriate safeguards.

16.1.4 ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

16.1.4.1 Developer action elements

16.1.4.1.1 ALC_DVS.1.1D

The developer shall produce development security documentation.

16.1.4.2 Content and presentation of evidence elements

16.1.4.2.1 ALC_DVS.1.1C

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

16.1.4.2.2 ALC_DVS.1.2C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

16.1.4.3 Evaluator action elements

16.1.4.3.1 ALC_DVS.1.1E

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

16.1.4.3.2 ALC_DVS.1.2E

The evaluator shall confirm that the security measures are being applied.

16.1.5 ALC_DVS.2 Sufficiency of security measures

Dependencies: No dependencies.

16.1.5.1 Developer action elements

16.1.5.1.1 ALC_DVS.2.1D

The developer shall produce development security documentation.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.1.5.2 Content and presentation of evidence elements

16.1.5.2.1 ALC_DVS.2.1C

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

16.1.5.2.2 ALC_DVS.2.2C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

16.1.5.2.3 ALC_DVS.2.3C

The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

16.1.5.3 Evaluator action elements

16.1.5.3.1 ALC_DVS.2.1E

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

16.1.5.3.2 ALC_DVS.2.2E

The evaluator shall confirm that the security measures are being applied.

16.2 Flaw remediation (ALC_FLR)

16.2.1 Objectives

Flaw remediation requires that discovered security flaws be tracked and corrected by the developer. Although future compliance with flaw remediation procedures cannot be determined at the time of the TOE evaluation, it is possible to evaluate the policies and procedures that a developer has in place to track and correct flaws, and to distribute the flaw information and corrections.

16.2.2 Component levelling

The components in this family are levelled on the basis of the increasing extent in scope of the flaw remediation procedures and the rigour of the flaw remediation policies.

16.2.3 Application notes

This family provides assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE. Additionally, requirements are included for the distribution of flaw corrections. However, this family does not impose evaluation requirements beyond the current evaluation.

The TOE user is considered to be the focal point in the user organisation that is responsible for receiving and implementing fixes to security flaws. This is not necessarily an individual user, but may be an organisational representative who is responsible for the handling of security flaws. The use of the term TOE user recognises that different organisations have different procedures for handling flaw reporting, which may be done either by an individual user, or by a central administrative body.

The flaw remediation procedures should describe the methods for dealing with all types of flaws encountered. These flaws may be reported by the developer, by users of the TOE, or by other parties with familiarity with the TOE. Some flaws may not be reparable immediately. There may be some occasions where a flaw cannot be fixed and other (e.g. procedural) measures must be taken. The documentation provided should cover the

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

procedures for providing the operational sites with fixes, and providing information on flaws where fixes are delayed (and what to do in the interim) or when fixes are not possible.

Once the evaluation of a TOE is complete, it is no longer the target for evaluation. Furthermore, any changes to this evaluated TOE result in the original evaluation results being no longer applicable to the changed version. The phrase release of the TOE used in this family therefore refers to a version of a product or system that is a release of a certified TOE, to which changes have been applied.

16.2.4 ALC_FLR.1 Basic flaw remediation

Dependencies: No dependencies.

16.2.4.1 Developer action elements

16.2.4.1.1 ALC_FLR.1.1D

The developer shall provide flaw remediation procedures addressed to TOE developers.

16.2.4.2 Content and presentation of evidence elements

16.2.4.2.1 ALC_FLR.1.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

16.2.4.2.2 ALC_FLR.1.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

16.2.4.2.3 ALC_FLR.1.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

16.2.4.2.4 ALC_FLR.1.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

16.2.4.3 Evaluator action elements

16.2.4.3.1 ALC_FLR.1.1E

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

16.2.5 ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies.

16.2.5.1 Objectives

In order for the developer to be able to act appropriately upon security flaw reports from TOE users, and to know to whom to send corrective fixes, TOE users need to understand how to submit security flaw reports to the developer. Flaw remediation guidance from the developer to the TOE user ensures that TOE users are aware of this important information.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.2.5.2 Developer action elements

16.2.5.2.1 ALC_FLR.2.1D

The developer shall provide flaw remediation procedures addressed to TOE developers.

16.2.5.2.2 ALC_FLR.2.2D

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

16.2.5.2.3 ALC_FLR.2.3D

The developer shall provide flaw remediation guidance addressed to TOE users.

16.2.5.3 Content and presentation of evidence elements

16.2.5.3.1 ALC_FLR.2.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

16.2.5.3.2 ALC_FLR.2.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

16.2.5.3.3 ALC_FLR.2.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

16.2.5.3.4 ALC_FLR.2.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

16.2.5.3.5 ALC_FLR.2.5C

The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

16.2.5.3.6 ALC_FLR.2.6C

The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

16.2.5.3.7 ALC_FLR.2.7C

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

16.2.5.3.8 ALC_FLR.2.8C

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.2.5.4 Evaluator action elements

16.2.5.4.1 ALC_FLR.2.1E

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

16.2.6 ALC_FLR.3 Systematic flaw remediation

Dependencies: No dependencies.

16.2.6.1 Objectives

In order for the developer to be able to act appropriately upon security flaw reports from TOE users, and to know to whom to send corrective fixes, TOE users need to understand how to submit security flaw reports to the developer, and how to register themselves with the developer so that they may receive these corrective fixes. Flaw remediation guidance from the developer to the TOE user ensures that TOE users are aware of this important information.

16.2.6.2 Developer action elements

16.2.6.2.1 ALC_FLR.3.1D

The developer shall provide flaw remediation procedures addressed to TOE developers.

16.2.6.2.2 ALC_FLR.3.2D

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

16.2.6.2.3 ALC_FLR.3.3D

The developer shall provide flaw remediation guidance addressed to TOE users.

16.2.6.3 Content and presentation of evidence elements

16.2.6.3.1 ALC_FLR.3.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

16.2.6.3.2 ALC_FLR.3.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

16.2.6.3.3 ALC_FLR.3.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

16.2.6.3.4 ALC_FLR.3.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.2.6.3.5 ALC_FLR.3.5C

The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

16.2.6.3.6 ALC_FLR.3.6C

The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

16.2.6.3.7 ALC_FLR.3.7C

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

16.2.6.3.8 ALC_FLR.3.8C

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

16.2.6.3.9 ALC_FLR.3.9C

The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

16.2.6.3.10 ALC_FLR.3.10C

The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

16.2.6.3.11 ALC_FLR.3.11C

The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

16.2.6.4 Evaluator action elements

16.2.6.4.1 ALC_FLR.3.1E

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

16.3 Life cycle definition (ALC_LCD)

16.3.1 Objectives

Poorly controlled development and maintenance of the TOE can result in a flawed implementation of a TOE (or a TOE that does not meet all of its security requirements). This, in turn, results in security violations. Therefore, it is important that a model for the development and maintenance of a TOE be established as early as possible in the TOE's life-cycle.

Using a model for the development and maintenance of a TOE does not guarantee that the TOE will be free of flaws, nor does it guarantee that the TOE will meet all of its security functional requirements. It is possible that the model chosen will be insufficient or inadequate and therefore no benefits in the quality of the TOE can be observed. Using a life-cycle model that has been approved by some group of experts (e.g. academic experts, standards bodies) improves the chances that the development and maintenance models will contribute to the overall quality of the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.3.2 Component levelling

The components in this family are levelled on the basis of increasing requirements for standardisation and measurability of the life-cycle model, and for compliance with that model.

16.3.3 Application notes

A life-cycle model encompasses the procedures, tools and techniques used to develop and maintain the TOE. Aspects of the process that may be covered by such a model include design methods, review procedures, project management controls, change control procedures, test methods and acceptance procedures. An effective life-cycle model will address these aspects of the development and maintenance process within an overall management structure that assigns responsibilities and monitors progress.

Although life-cycle definition deals with the maintenance of the TOE and hence with aspects becoming relevant after the completion of the evaluation, its evaluation adds assurance through an analysis of the life-cycle information for the TOE provided at the time of the evaluation.

A standardised life-cycle model is a model that has been approved by some group of experts (e.g. academic experts, standards bodies).

A measurable life-cycle model is a model with arithmetic parameters and/or metrics that measure TOE development properties (e.g. source code complexity metrics).

A life-cycle model provides for the necessary control over the development and maintenance of the TOE, if the developer can supply information that shows that the model appropriately minimises the danger of security violations in the TOE. Information given in the ST about the intended environment of the TOE and about the TOE's security objectives may be useful in defining the model for the portion of the life-cycle after the delivery of the TOE.

16.3.4 ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

16.3.4.1 Developer action elements

16.3.4.1.1 ALC_LCD.1.1D

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

16.3.4.1.2 ALC_LCD.1.2D

The developer shall provide life-cycle definition documentation.

16.3.4.2 Content and presentation of evidence elements

16.3.4.2.1 ALC_LCD.1.1C

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

16.3.4.2.2 ALC_LCD.1.2C

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.3.4.3 Evaluator action elements

16.3.4.3.1 ALC_LCD.1.1E

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

16.3.5 ALC_LCD.2 Standardised life-cycle model

Dependencies: No dependencies.

16.3.5.1 Developer action elements

16.3.5.1.1 ALC_LCD.2.1D

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

16.3.5.1.2 ALC_LCD.2.2D

The developer shall provide life-cycle definition documentation.

16.3.5.1.3 ALC_LCD.2.3D

The developer shall use a standardised life-cycle model to develop and maintain the TOE.

16.3.5.2 Content and presentation of evidence elements

16.3.5.2.1 ALC_LCD.2.1C

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

16.3.5.2.2 ALC_LCD.2.2C

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

16.3.5.2.3 ALC_LCD.2.3C

The life-cycle definition documentation shall explain why the model was chosen.

16.3.5.2.4 ALC_LCD.2.4C

The life-cycle definition documentation shall explain how the model is used to develop and maintain the TOE.

16.3.5.2.5 ALC_LCD.2.5C

The life-cycle definition documentation shall demonstrate compliance with the standardised life-cycle model.

16.3.5.3 Evaluator action elements

16.3.5.3.1 ALC_LCD.2.1E

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.3.6 ALC_LCD.3 Measurable life-cycle model

Dependencies: No dependencies.

16.3.6.1 Developer action elements

16.3.6.1.1 ALC_LCD.3.1D

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

16.3.6.1.2 ALC_LCD.3.2D

The developer shall provide life-cycle definition documentation.

16.3.6.1.3 ALC_LCD.3.3D

The developer shall use a standardised **and measurable** life-cycle model to develop and maintain the TOE.

16.3.6.1.4 ALC_LCD.3.4D

The developer shall measure the TOE development using the standardised and measurable life-cycle model.

16.3.6.2 Content and presentation of evidence elements

16.3.6.2.1 ALC_LCD.3.1C

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE, **including the details of its arithmetic parameters and/or metrics used to measure the TOE development against the model.**

16.3.6.2.2 ALC_LCD.3.2C

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

16.3.6.2.3 ALC_LCD.3.3C

The life-cycle definition documentation shall explain why the model was chosen.

16.3.6.2.4 ALC_LCD.3.4C

The life-cycle definition documentation shall explain how the model is used to develop and maintain the TOE.

16.3.6.2.5 ALC_LCD.3.5C

The life-cycle definition documentation shall demonstrate compliance with the standardised **and measurable** life-cycle model.

16.3.6.2.6 ALC_LCD.3.6C

The life-cycle documentation shall provide the results of the measurements of the TOE development using the standardised and measurable life-cycle model.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.3.6.3 Evaluator action elements

16.3.6.3.1 ALC_LCD.3.1E

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

16.4 Tools and techniques (ALC_TAT)

16.4.1 Objectives

Tools and techniques is an aspect of selecting tools that are used to develop, analyse and implement the TOE. It includes requirements to prevent ill-defined, inconsistent or incorrect development tools from being used to develop the TOE. This includes, but is not limited to, programming languages, documentation, implementation standards, and other parts of the TOE such as supporting runtime libraries.

16.4.2 Component levelling

The components in this family are levelled on the basis of increasing requirements on the description and scope of the implementation standards and the documentation of implementation- dependent options.

16.4.3 Application notes

There is a requirement for well-defined development tools. These are tools that have been shown to be applicable without the need for intensive further clarification. For example, programming languages and computer aided design (CAD) systems that are based on an a standard published by standards bodies are considered to be well-defined.

Tools and techniques distinguishes between the implementation standards applied by the developer (ALC_TAT.2.3D) and the implementation standards for “all parts of the TOE” (ALC_TAT.3.3D) that additionally includes third party software, hardware, or firmware.

The requirement in ALC_TAT.1.2C is especially applicable to programming languages so as to ensure that all statements in the source code have an unambiguous meaning.

16.4.4 ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Subset of the implementation of the TSF

16.4.4.1 Developer action elements

16.4.4.1.1 ALC_TAT.1.1D

The developer shall identify the development tools being used for the TOE.

16.4.4.1.2 ALC_TAT.1.2D

The developer shall document the selected implementation-dependent options of the development tools.

16.4.4.2 Content and presentation of evidence elements

16.4.4.2.1 ALC_TAT.1.1C

All development tools used for implementation shall be well-defined.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.4.4.2.2 ALC_TAT.1.2C

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

16.4.4.2.3 ALC_TAT.1.3C

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

16.4.4.3 Evaluator action elements

16.4.4.3.1 ALC_TAT.1.1E

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

16.4.5 ALC_TAT.2 Compliance with implementation standards

Dependencies: ADV_IMP.1 Subset of the implementation of the TSF

16.4.5.1 Developer action elements

16.4.5.1.1 ALC_TAT.2.1D

The developer shall identify the development tools being used for the TOE.

16.4.5.1.2 ALC_TAT.2.2D

The developer shall document the selected implementation-dependent options of the development tools.

16.4.5.1.3 ALC_TAT.2.3D

The developer shall describe the implementation standards to be applied.

16.4.5.2 Content and presentation of evidence elements

16.4.5.2.1 ALC_TAT.2.1C

All development tools used for implementation shall be well-defined.

16.4.5.2.2 ALC_TAT.2.2C

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

16.4.5.2.3 ALC_TAT.2.3C

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

16.4.5.3 Evaluator action elements

16.4.5.3.1 ALC_TAT.2.1E

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

16.4.5.3.2 ALC_TAT.2.2E

The evaluator shall confirm that the implementation standards have been applied.

16.4.6 ALC_TAT.3 Compliance with implementation standards - all parts

Dependencies: ADV_IMP.1 Subset of the implementation of the TSF

16.4.6.1 Developer action elements

16.4.6.1.1 ALC_TAT.3.1D

The developer shall identify the development tools being used for the TOE.

16.4.6.1.2 ALC_TAT.3.2D

The developer shall document the selected implementation-dependent options of the development tools.

16.4.6.1.3 ALC_TAT.3.3D

The developer shall describe the implementation standards **for all parts of the TOE.**

16.4.6.2 Content and presentation of evidence elements

16.4.6.2.1 ALC_TAT.3.1C

All development tools used for implementation shall be well-defined.

16.4.6.2.2 ALC_TAT.3.2C

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

16.4.6.2.3 ALC_TAT.3.3C

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

16.4.6.3 Evaluator action elements

16.4.6.3.1 ALC_TAT.3.1E

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

16.4.6.3.2 ALC_TAT.3.2E

The evaluator shall confirm that the implementation standards have been applied.

17 Class ATE: Tests

The class “Tests” encompasses four families: coverage (Coverage (ATE_COV)), depth (Depth (ATE_DPT)), independent testing (e.g. functional testing performed by evaluators) (Independent testing (ATE_IND)), and functional tests (Functional tests (ATE_FUN)). Testing helps to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified. Testing may also be directed toward the internal structure of the TSF, such as the testing of subsystems and modules against their specifications.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

The aspects of coverage and depth have been separated from functional tests for reasons of increased flexibility in applying the components of the families. However, the requirements in these three families are intended to be applied together.

The independent testing family has dependencies on the other families to provide the necessary information to support the requirements, but is primarily concerned with independent evaluator actions.

The emphasis in this class is on confirmation that the TSF operates according to its specification. This will include both positive testing based on functional requirements, and negative testing to check that undesirable behaviour is absent. This class does not address penetration testing, which is directed toward finding vulnerabilities that enable a user to violate the security policy. Penetration testing is based upon an analysis of the TOE that specifically seeks to identify vulnerabilities in the design and implementation of the TSF, and is addressed separately as an aspect of vulnerability assessment in the class AVA: Vulnerability assessment.

Figure 14 shows the families within this class, and the hierarchy of components within the families.

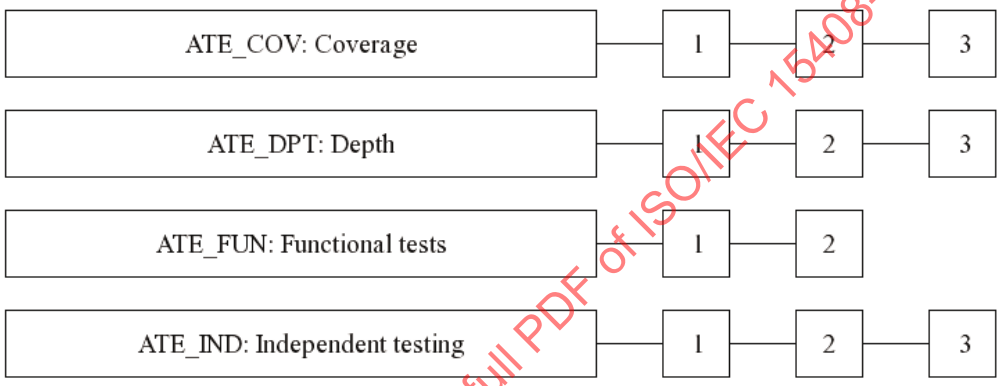


Figure 14 - ATE: Tests class decomposition

17.1 Coverage (ATE_COV)

17.1.1 Objectives

This family addresses those aspects of testing that deal with completeness of test coverage. That is, it addresses the extent to which the TSF is tested, and whether or not the testing is sufficiently extensive to demonstrate that the TSF operates as specified.

17.1.2 Component levelling

The components in this family are levelled on the basis of increasing rigour of interface testing, and increasing rigour of the analysis of the sufficiency of the tests to demonstrate that the TSF operates in accordance with its functional specification.

17.1.3 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.1 Informal functional specification

ATE_FUN.1 Functional testing

17.1.3.1 Objectives

In this component, the objective is to establish that the TSF has been tested against its functional specification. This is to be achieved through an examination of developer evidence of correspondence.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

17.1.3.2 Application notes

While the testing objective is to cover the TSF, there is no requirement to provide anything to verify this assertion other than an informal mapping of tests to the functional specification and the testing data itself.

In this component the developer is required to show how the tests that have been identified correspond to the TSF as described in the functional specification. This can be achieved by a statement of correspondence, perhaps using a table. This information is required to support the evaluator in planning the test programme for the evaluation. At this level there is no requirement for complete coverage of every aspect of the TSF by the developer, and the evaluator will need to take account of any deficiencies in this area.

17.1.3.3 Developer action elements

17.1.3.3.1 ATE_COV.1.1D

The developer shall provide evidence of the test coverage.

17.1.3.4 Content and presentation of evidence elements

17.1.3.4.1 ATE_COV.1.1C

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

17.1.3.5 Evaluator action elements

17.1.3.5.1 ATE_COV.1.1E

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

17.1.4 ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.1 Informal functional specification

ATE_FUN.1 Functional testing

17.1.4.1 Objectives

In this component, the objective is to establish that the TSF has been tested against its functional specification in a systematic manner. This is to be achieved through an examination of developer analysis of correspondence.

17.1.4.2 Application notes

The developer is required to demonstrate that the tests which have been identified include testing of all of the security functions as described in the functional specification. The analysis should not only show the correspondence between tests and security functions, but should provide also sufficient information for the evaluator to determine how the functions have been exercised. This information can be used in planning for additional evaluator tests. Although at this level the developer has to demonstrate that each of the functions within the functional specification has been tested, the amount of testing of each function need not be exhaustive.

17.1.4.3 Developer action elements

17.1.4.3.1 ATE_COV.2.1D

The developer shall provide **an analysis** of the test coverage.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved

17.1.4.4 Content and presentation of evidence elements

17.1.4.4.1 ATE_COV.2.1C

The **analysis** of the test coverage shall **demonstrate** the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

17.1.4.4.2 ATE_COV.2.2C

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

17.1.4.5 Evaluator action elements

17.1.4.5.1 ATE_COV.2.1E

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

17.1.5 ATE_COV.3 Rigorous analysis of coverage

Dependencies: ADV_FSP.2 Fully defined external interfaces

ATE_FUN.1 Functional testing

17.1.5.1 Objectives

In this component, the objective is to establish that the TSF has been tested against its functional specification in a systematic and exhaustive manner. This is to be achieved through an examination of developer analysis of correspondence.

17.1.5.2 Application notes

The developer is required to provide a convincing argument that the tests which have been identified cover all security functions, and that the testing of each security function is complete. There will remain little scope for the evaluator to devise additional functional tests of the TSF interfaces based on the functional specification, as they will have been exhaustively tested. Nevertheless, the evaluator should strive to devise such tests.

17.1.5.3 Developer action elements

17.1.5.3.1 ATE_COV.3.1D

The developer shall provide an analysis of the test coverage.

17.1.5.4 Content and presentation of evidence elements

17.1.5.4.1 ATE_COV.3.1C

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

17.1.5.4.2 ATE_COV.3.2C

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-3:2005

© ISO/IEC 2005 - All rights reserved